An existential crisis *and* a golden opportunity? Assessing hard-target espionage in the cyber era

Kyle S. Cunliffe

Thesis submitted in fulfilment of the requirements for the degree of PhD

Department of International Politics
Aberystwyth University
January 18th 2021

Summary

Cyberspace is transforming global society. Its effects on states, intelligence, and national security are the subject of much comment, but its relationship with espionage, or human intelligence, remains under-researched to an alarming degree. At a time when the British-US intelligence community is making headway in cyberspace, necessitated by emerging threats and rising nation-state agendas, this is a glaring omission. The strategic imperatives of Russia and China have provoked a reorientation by the British SIS and the US CIA, turning resources back towards nation-state 'hard targets'. Yet these hard target states are investing resources in innovative surveillance practices, tools that fundamentally threaten intelligence officers' ability to travel freely or acquire the increasingly important human sources (agents) of espionage. As the operations of British-US intelligence personnel become more threatened in physical terms, espionage agencies now focus their attention towards cyberspace, where innovation opens up new opportunities in tradecraft. By turning to cyberspace to conduct tradecraft, particularly in the recruitment and handling of spies, espionage's success and failure is now entwined with the value of innovation, and as consequence, cyber-enabled tradecraft is entwined with the present and future of Western security. However, the value of cyberspace to espionage's sources and methods remains ambiguous, receiving only limited study. Views put forward by a small cadre of mostly seasoned practitioners, express both powerful enthusiasm and debilitating cynicism, reflecting a dichotomy of opinions that have not yet been addressed. No one has yet sought to fully determine the value of cyberspace to espionage when conducted against a hard-target state, where the Internet is subject to the full weight of counterintelligence. This thesis therefore explores the merits of cyberspace to espionage tradecraft, in the context of its value applied toward Russia and China. It uses Cold War history as a basis for drawing abductive hypotheses, turning to the first era of major innovation in espionage affairs, the mid-Cold War period, for guidance in understanding the present period of innovation. In turn, it will explore how this overt technology, used for covert means, carries significant limitations to the purposes of spying, specifically due to technology's relationship with human behaviour, thus incurring wider consequences for the future of intelligence collection, and concurrently, national security.

Contents

Acknowledgements

Akin to any spy, this thesis would not have been possible without a network of supporting, tolerant, and very patient collaborators. It would certainly not exist without the open-mindedness of my recruiters, the agency who ensnared my life for the better part of a decade – the University of Aberystwyth, and its sterling Department of International Politics. My gratitude for receiving the E.H. Carr scholarship cannot be understated, and I will be forever thankful for this opportunity. Nor would it exist without my army of handlers throughout the years, most notably Gerald R. Hughes and Kris Stoddart, whose supervision, wisdom, and guidance have been invaluable. In particular, I would like to thank Gerald R. Hughes, for giving me the freedom to pursue my wild ideas, and for his eternal, straight-talking insights - steering me back on track on more than one occasion. I would also extend a great deal of thanks to Kris Stoddart, who continued to offer advice and wisdom long after his supervisory obligations had passed – and for reassuring me that my mad ideas were perhaps not as crazy as I presupposed.

But all wild plans need an inspiration, and to that, I am forever indebted to my former Station Chief, the Yoda of espionage, Len Scott. His teaching during my Masters' years cemented my passion for the mysterious world of human intelligence, a passion that flourished as Len's student and later assistant tutor in his *Espionage* module. It was a great pleasure to turn the deceptive tricks he played on me on and my comrades against fresh and unwitting undergraduates. Without Len's encouragement, including his teachings on the murky world of espionage and tradecraft, or his mind games involving an octopus and a fez, I don't believe this thesis would ever have come to be. Aberystwyth Station is, however, only a resounding success through the aid of its tireless support staff, and my appreciation goes out to Vicki Jones, Donia Richards, Elaine Lowe, Glesni Davies, and many others.

I offer enormous thanks to my current colleagues at Salford University, and especially to Christopher Murphy, for his tireless support, patience, and input. Moreover, no operation is ever complete without the wisdom of seasoned practitioners. I would therefore like to express particular gratitude to former CIA officers David Gioe and Robert Wallace. The insights they offered via interviews and conversations were greatly appreciated, providing a guiding hand for the direction of this project. I also hold much gratitude to my serving and former agents of the Interpol department, to the men and women who journeyed down the baffling world of the PhD alongside me, and who's kinship (and many beers) kept me sane and determined, including Charlotte Botfield, Bleddyn Bowen, Jessica Sheehan, Kris Lovell, Chris Smith, Desiree Poets, and many, many more. Bleddyn's advice throughout the years has also been most helpful, and I greatly appreciate his reviewing of my work and constructive feedback. I also extend my gratitude to former colleagues (and friends) of Aberystwyth's Residential Tutor department, who's antics and hard-work passed the long summer months (and forever improved my cocktail-smithing skills.) And I offer a great deal of thanks to Alex da Costa, of Cambridge University, whose proofreading skills flagged up more than a typo or two (an understatement by any measure).

And finally, I have endless gratitude to my family and friends, who have kept me grounded, loved, supported and encouraged throughout this journey. Without the endless support of my parents, grandparents, and eclectic range of strange and unusual friends, this thesis would never have neared completion. Particular thanks go out to my grandfather, Joseph Forshaw, whom I will forever miss, and to my mother, for her tireless patience in putting up with me for all these years.

Recurring abbreviations:

CCP – Chinese Communist Party
CCTV – Closed Circuit Television
CI – Counterintelligence
CIA – Central Intelligence Agency (US)
DDI – Directorate of Digital Innovation
JTRIG – Joint Threat Intelligence Group
DoD – Department of Defense (US)
DPI – Deep packet inspection
EU – European Union
FBI – Federal Bureau of Investigation (US)
FSB – Federal Security Service of the Russian Federation
GCHQ – Government Communications Headquarters (UK)
GRU – Soviet & Russian Federation Military Intelligence.
HUMINT – Human Intelligence
KGB – Foreign and Domestic intelligence service of the Soviet Union.
MI5 – Military Intelligence Five / The Security Service (UK)
MSS – Ministry of State Security (China)
NATO – North Atlantic Treaty Organisation
NSA – National Security Agency (US)
OPM – Office of Personnel Management (US)
OSINT – Open Source Intelligence
OTS – Office of Technical Services (CIA)
SIGINT – Signals Intelligence
SIS – Secret Intelligence Service (UK)
SRAC – Short-range agent communications device.
SVR – Russian Federation Foreign Intelligence
TECHINT – Technical Intelligence
TSD – Technical Services Division (CIA)

AN EXISTENTIAL CRISIS *AND* A GOLDEN OPPORTUNITY?:
Assessing hard-target espionage in the cyber era

Introduction
A feasible solution?

Espionage, or what is more often known as human intelligence, is fundamentally about people, yet this dissertation aims to assess its relationship with cyberspace. Merely convincing a foreign official to walk a path that too often ends in execution or imprisonment is a delicate task, while the personal foibles which intelligence officers exploit to recruit spies are just as likely to sow the seeds of distrust and doubt.[1] As such, at the heart of spying lies the trusting bonds between those who spy and the operatives who enable them.[2] Those bonds, as with all relationships, are best developed face-to-face, but personal meetings are 'almost always the most precarious and dangerous part' of any operation.[3] In the past, the perils of street surveillance, meaning the observation of foreign intelligence officers, led to new innovations in 'tradecraft', the methods used to recruit and handle spies.[4] But as the espionage world enters into a changing security landscape, one defined by a new age of street surveillance threats, innovation is rising up the agenda.[5][6] This thesis is thus a study of cyber-enabled tradecraft, as a solution to a problem that intelligence officers cannot ignore.

[1] Wilder, U. M. 'The psychology of espionage', *Studies in Intelligence, CIA,* 61:2, 2017, p. 19-34; Burkett, R. 'Rethinking an old approach: an alternative framework for agent recruitment: from MICE to RASCLS', *Studies in Intelligence, CIA,* 57:1, 2013, p. 7-17.
[2] Gioe, D. V. 'The more things change': HUMINT in the cyber age', in *The Palgrave Handbook of Security, Risk and Intelligence*, edited by Robert Dover, Huw Dylan, and Michael Goodman (London, Palgrave, Macmillan, 2017), p. 221-222.
[3] Ibid, p. 220.
[4] Wallace, R. et al. *Spycraft: inside the CIA's top secret spy lab,* (London, Bantam Press, 2008), p. 36-40
[5] This transformation was outlined in a lengthy speech by the Deputy Director of the CIA in 2015, David S. Cohen, which set out the agency's role, challenges, and evolution in the digital world. For more details see: CIA (18 September 2015) Deputy Director Cohen delivers remarks on CIA of the future at Cornell University. Available at: https://www.cia.gov/news-information/speeches-testimony/2015-speeches-testimony/deputy-director-cohen-delivers-remarks-on-cia-of-the-future-at-cornell-university.html [accessed 10 January 2018].
[6] See APPENDIX 1 for a full transcript of Cohen's speech.

Tradecraft is often regarded as more of an art than a science, 'a combination of common sense and imagination'.[7] The CIA even recruited magician, John Mulholland, to write tradecraft manuals using established theories of deception.[8] But common sense and imagination are not enough to overcome the challenges of hard-target states, meaning intelligence officers must make "wise decisions about what tools, materials, and processes to apply to their work."[9] This was exemplified in the Cold War, where Moscow's 'hard target' conditions forced intelligence agencies to rethink the tried and tested methods of the past.[10] It kickstarted a cultural transformation, whereby for the first time in history, technology's role in espionage shifted from a minor role, to a vital function in operational affairs.[11] Yet, while twentieth century technologies opened doors, Western espionage never reclaimed any significant advantage over the Soviet KGB.[12] This brief history lesson is important, because while the Cold War has ended, today's practitioners face a new hard target problem.

This 'hard target problem' begins with the changing landscape of international relations, as the world edges closer to what some pundits are calling the 'new Cold War'.[13] In 2015, the UK government outlined concerns about the 'resurgence of state-based threats', listing, above all other states, 'Russian behaviour' as a current and long-term priority.[14] Washington echoed these sentiments in 2015, accusing the Kremlin of

[7] Holm, R. *The craft we chose: my life in the CIA,* (Oakland, Mountain Lake Press, 2011), p. 275.
[8] Wallace, R. & Melton, H. K. *C.I.A. manual of trickery and deception,* (London, Harper Collins, 2009), p. 15.
[9] Email correspondence with Robert Wallace, co-author of *Spycraft*, by Kyle Cunliffe, 2015.
[10] Wallace, R. et al. *Spycraft*, p. 36-40.
[11] Ibid.
[12] Russel, R. L. *Sharpening strategic intelligence: why the CIA gets it wrong and what needs to be done to get it right*, [Kindle version] (New York, Cambridge University Press, 2007), p. 51-52.
[13] Lucas, E. *Deception: Spies, lies, and how Russia dupes the West,* (London, Bloomsbury Publishing PLC, 2013), p. 16.
[14] HM Government (November 2015) National security strategy and strategic defence and security review 2015, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf [accessed 31 October 2017], p. 18.

endangering 'international norms that have largely been taken for granted since the end of the Cold War'.[15] But unlike the first Cold War, the current security climate is no longer dominated by a single monolithic threat.[16] Although Putin's Russia boasts many parallels with its former Soviet self, not least enormous nuclear prowess, Russia is now arguably the lesser concern, dwarfed by the prospects of conflict with a rising China.[17] Subsequently, despite mounting problems posed by North Korea, Iran, ISIS, Syria, and a plethora of evolving threats, Russia and China are considered the primary challengers to 'American power, influence and interests'.[18]

However, as the West turns its defence and intelligence institutions back towards nation-states, espionage must play an increasingly important role. Contrary to outdated contentions that espionage would decline in the face of emerging technical intelligence methods, human agents offer an invaluable pathway to secrets that cannot be gleaned by other means.[19] In a move indicative of the spy's continued relevance, in 2016 the UK's chief espionage agency, SIS, received a substantial increase in funding, to bolster its personnel by forty percent.[20] And yet, it seems SIS's growth echoed an

[15] The White House (February 2015) National Security Strategy. Available at: https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf [accessed 20 July 2017], p. 10.
[16] Office of the Director of National Intelligence (13 February 2018) Statement for the record: worldwide threat assessment of the US intelligence community. Available at: https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1845-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community [accessed 12 June 2018].
[17] McGreal, C. (9 March 2016) America's former CIA chief: 'If we don't handle China well, it will be catastrophic', *The Guardian.* Available from https://www.theguardian.com/us-news/2016/mar/09/america-cia-nsa-chief-general-michael-hayden-china-catastrophic-for-world [accessed 12 October 2020].
[18] Office of the Director of National Intelligence (11 May 2017) Worldwide threat assessment of the US Intelligence Community. Available at: https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf [accessed 15 January 2018]; White House (December 2017) National Security Strategy. Available at: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf [accessed 1 February 2018], p. 3.
[19] CIA (18 September 2015) Deputy Director Cohen delivers remarks on CIA of the future at Cornell University. Available at: https://www.cia.gov/news-information/speeches-testimony/2015-speeches-testimony/deputy-director-cohen-delivers-remarks-on-cia-of-the-future-at-cornell-university.html [accessed 1 January 2018].
[20] BBC News (21 September 2016) MI6 set to recruit 1,000 extra staff. Available at: https://www.bbc.co.uk/news/uk-37434131 [accessed 1 December 2016].

underlying issue, which stands as the very impetus for this study. According to media reports, it was motivated by necessity, as the threat of technologically-augmented street surveillance now looms over espionage's future.[21] Surveillance in these countries is an established norm, yet aided by emerging technologies, it is quickly eroding the modern operative's ability to maintain their cover and escape the pervasive glare of their watchers. The proliferation of biometric checkpoints permanently ties identities to a single passport, while a person's background can be rapidly checked against mounting records of 'life history data'.[22] Resultantly, as hard targets rise up the agenda, the operational threats to espionage continue to mount, posing serious consequences if new means cannot be found to recruit or handle spies.

But according to Alex Younger, the former chief of SIS, espionage in the cyber era faces not just an "existential threat", but also a "*golden opportunity*".[23] Scholars and intelligence practitioners argue that by harnessing the benefits of 'cyber power', new tradecraft can be developed to recruit and handle spies, reducing, or even eliminating, the need for face-to-face meetings.[24] The CIA's determination to improve its cyber-enabled tradecraft became clear in 2015, revealing its first new directorate in over fifty years, *The Directorate of Digital Innovation,* for the purpose of researching and identifying technological threats and opportunities.[25] This is not an encroachment on the turf of NSA, but rather an effort to harness technology for espionage purposes, as the then serving CIA Director argued, "human interactions take place in that digital domain. So the intelligence profession needs to flourish in that domain. It cannot avoid

[21] Ibid.
[22] Clark, R. *Intelligence collection,* (Thousand Oaks, CQ Press, 2014), p. 60.
[23] GW Center for Cyber and Homeland Security (21 September 2016) CIA-GW intelligence conference: Panel on the view from foreign intelligence chiefs, *Youtube*. Available at: https://www.youtube.com/watch?v=yefBv7Q3sv0 [accessed 11 January 2018].
[24] Gioe, D. V. 'The more things change', p. 217
[25] Defense One (6 March 2015) CIA restructuring adds new cyber focus. Available at: http://www.defenseone.com/technology/2015/03/cia-restructuring-adds-new-cyber-focus/106953/ [accessed 11 January 2018]

it."[26] Sceptics, on the other hand, contend that technological tradecraft is inherently insecure, and vulnerable to the foibles of human behaviour.[27] Their concerns were echoed in 2018, following headlines claiming that swathes of CIA agents were arrested inside China and Iran, because an online covert communications system was exposed by a duplicitous Iranian asset.[28] As a consequence, espionage's future, alongside the utility of intelligence in supporting policymakers decisions, hinges on the value of cyber-enabled tradecraft, a value that is currently opaque.

To what extent cyberspace will provide espionage practitioners the edge they require to pierce these hard target states is thus the query of this study. In turn, this dissertation presupposes that human behaviour determines the outcome of tradecraft's success or failure, on the logic that all espionage is ultimately dependent on the behaviour of the third party, the prospective or serving spy. Therefore, although technology evolves over time, this study seeks to show that in hard target conditions, tradecraft's success is constricted by a rising need for trust, in people and technology - trust that is difficult to establish in the absence of secure tradecraft. But since intelligence's sources and methods languish in the shadows of official secrecy, it aims to prove this argument through an abductive model.[29] Hence, it will draw 'speculative hypotheses' from history, to be tested against the cyber evidence, 'rather as doctors do as they test out different diagnoses.'[30] This is significant on three counts. First, it offers

[26] Reuters (2 November 2016) Digitizing the CIA: John Brennan's attempt to lead America's spies into the age of cyberwar. Available at: https://www.reuters.com/investigates/special-report/usa-cia-brennan/ [accessed 1 December 2016].
[27] Sano, J. 'The changing shape of HUMINT', *Intelligencer,* 21:3, 2015, p. 79; Tucker, D. *End of intelligence: Espionage and state power in the information age,* (Palo Alto, Stanford University Press, 2014), p.76.
[28] Yahoo News (2 November 2018) The CIA's communications suffered a catastrophic compromise. It started in Iran. Available at: https://in.news.yahoo.com/cias-communications-suffered-catastrophic-compromise-started-iran-090018710.html?guccounter=1 [accessed 3 November 2018].
[29] Gill, P. 'Theories of intelligence', in *The Oxford Handbook of National Security Intelligence, edited by Loch K. Johnson,* (Oxford, Oxford University Press, 2010), p. 44.
[30] Ibid.

a narrow window into the changing landscape of international relations, by determining whether espionage is equipped to meet policymakers needs. Second, it fills a significant gap in a severely understudied literature. Despite a small body of scholarship on cyberspace's assumed tradecraft *benefits*, this study can find no literature that has critically assessed its *limitations*. Third, although this dissertation focuses on British / US espionage, on account of data availability and political prescience, an abductive model bestows lessons which can be universally applied, relevant to tradecraft's developments, and all actors who use them, in the past, present, and future.

Chapter one sets out the concepts, literature, and methodology underpinning this dissertation. It compiles the literature's various and often haphazard musings on cyber tradecraft into two polarised camps. First, the *optimists* who see cyberspace as carrying profound implications to espionage, either as a positive force for Western intelligence or as a dangerous advantage for the West's competitors, and second, the *pessimists*, who see technology as inherently insecure. Crucially, it sets out a pathway for further research by identifying the key cyber developments which appear to pose the most significance to tradecraft's functions. These functions are essentially the important operational elements tradecraft needs to achieve, and they, along with their perceived cyber benefits, can be listed as follows:

> Recruitment: Intelligence officers can cultivate prospective agents through socially innocuous communications, including social networks, Internet forums and video games, or sources can volunteer their services online.
>
> Surveillance: Intelligence officers can 'spot' and 'assess' prospective agents by collecting personal information through online open sources, such as social media, or targeted hacking.
>
> Handling: Intelligence officers can manage and support serving agents with the aid of encrypted online covert communications (e.g. encrypted email) and anonymising tools such as The Onion Router.
>
> Collection: Intelligence officers can enable agents to collect their intelligence through microelectronic storage devices and malicious software (malware).

> These can be uploaded onto systems and automatically collect information on the agent's behalf, transmitting it via the Internet.

This is followed by a methodology that establishes an abductive model for further research, through an assessment of its strengths, limitations, and predictive capacity. Chapter two establishes the importance of espionage against Russia and China, honing on key issues such as military and nuclear modernisation, tensions in the Pacific and Eastern Europe, and aggressive intelligence activities. This analysis is drawn from policy reports and security themes, and conceptually examines the merits that espionage brings to intelligence's requirements. Chapter three narrows the lens to the rising threat of technologically-augmented street surveillance in Moscow and Beijing, weaving intelligence and counterintelligence concepts with mounting empirical evidence, to show how contemporary operational environments severely impact the feasibility of personal meetings. It concludes by examining the public responses of intelligence leaders, who propose that cyber-enabled tradecraft may offer the solutions espionage requires to overcome these emerging threats. Combined, they establish why hard-target espionage is both rising in importance, but also concurrently more difficult to achieve, ergo defining the problem to be addressed.

Chapter four provides a framework for determining why tradecraft succeeds or fails. With an analysis of situational parallels drawn from an extensive body of literature, it presents the case for using British / US espionage against the Soviet Union in the mid-late Cold War, as the basis for an abductive analysis. Following the four functions of tradecraft identified in the literature review, it draws on the trials and errors of espionage throughout this era, with the intent to determine why tradecraft succeeded or failed. By conceptually exploring the operational strengths and limits of tradecraft throughout these four functions, supported by applied examples where possible, it

develops the connection between risk and behaviour. It shows that as the risks pursuant to tradecraft rise, so too does the need to trust the behaviour of the prospective or serving spy, a factor that steers tradecraft's outcome towards pessimistic outcomes within hard targets conditions, where trust is most difficult to develop.

Chapters five and six use these abductive findings to assess the probabilistic outcomes of cyberspace in the four functions of tradecraft. This is achieved by interweaving, analysing, and adapting data pursuant to cyberspace's limitations in the context of hard target states. Chapter five begins with recruitment, examining the logical presumption that online social communications and intelligence agency websites could be used to cultivate and acquire prospective agents. This follows with *surveillance*, by examining the prospects of prying into the private affairs of foreign officials through open sources and hacking, to aid in the spotting and assessment of recruitment targets. In chapter six, tradecraft is examined from the point where a pre-existing intelligence connection exists between the parties, beginning with the impact of online covert communications on handling. This follows with an assessment of collection, examining the agent's ability to extract secret information from classified networks through microelectronic storage devices and malicious software. Throughout, it is shown that cyberspace is highly susceptible to counterintelligence threats, meaning intelligence officers will increasingly need to weigh the hazards of cyber-enabled tradecraft against the likelihood that their target, or agent, will behave in a manner that facilitates a positive outcome. This focus on human behaviour will be shown to be key, as with a reduced ability to meet sources face to face, which is a necessary means of determining behavioural characteristics and developing trust, espionage faces mounting operational challenges.

Chapter 1
Concepts, literature, and methodology

Introduction

Having established the aim of this thesis, this chapter sets out to define key concepts, identify a gap in the literature, and develop a methodology for further research. In an era of intelligence that is increasingly complicated and multifaceted, terms such as ‘espionage’ and ‘spying’ have lost much of their original meaning. The first priority, therefore, is to clearly distinguish espionage from other forms of intelligence collection, and establish its uniqueness from the broader subcategory of human intelligence. These conceptual complications are further compounded by espionage’s relationship with cyberspace, not least due to the emergence of the term ‘cyber espionage’. Thus, it is necessary to clearly define cyberspace, distinguishing its connection with espionage from more commonly understood cyber concepts.

This is followed by the literature review, which hones the lens to the handful of scholars who have touched on cyberspace’s impact on espionage. It is shown that while the literature on tradecraft has steadily evolved, it is an understudied dimension of intelligence scholarship. Nonetheless, a small but unrefined body of work has considered its connection to cyberspace, with two notable camps - the *optimists*, who see cyberspace as carrying positive implications to espionage, and the *pessimists* who remain unconvinced. Through analysing these works, this chapter identifies prominent themes and sets out a trajectory for further investigation. This is proceeded by the methodology, wherein it is argued that the enduring barrier of official secrecy can be surmounted through an abductive model. It will demonstrate that abduction, despite

being a more limited form of reasoning, is the most suitable solution for interpreting a world that is otherwise unobservable, allowing scholars to draw probabilistic outcomes through lessons drawn from intelligence's history.

Key intelligence concepts

In a CIA study, Bimfort asserted that defining intelligence was akin to 'making a microscopic portrait of a continent', because '[each] expert tends to view the term through the spectacles of his speciality'.[1] Any 'worthwhile' definition must incorporate a broad spectrum of activities, from collection and analysis, to counterintelligence and covert action.[2] But while no unanimous definitions exists, it 'may be best understood as a process by which competitors improve their decision-making relative to their opponents.'[3] Through the collection, processing, analysis, and dissemination of information (concertedly known as the "intelligence cycle"), decisionmakers can strengthen their own hand while minimising the threat of surprise.[4] It is information upon which states and their leaders rely to maintain and enhance security, offering enormous value to those willing to foot the bill.[5]

Intelligence, however, cannot succeed without collection. Intelligence failures can arise at any point in the intelligence cycle; even if good information is made available, analysts can draw misleading interpretations, and policymakers are under no obligations to heed their findings.[6] But fundamentally, analysts cannot misinterpret and

[1] Bimfort, M. T. 'A definition of intelligence', *Studies in Intelligence, CIA,* 2:2, 1958, p. 76.
[2] Gill, P. & Phythian, M. *Intelligence in an insecure world,* (Cambridge, Polity Press 2006), p. 1
[3] Sims, J. 'Defending adaptive realism: intelligence theory comes of age', *Intelligence theory*, edited by Peter Gill, Stephen Marrin, and Mark Phythian, (London, Routledge 2009), p. 161.
[4] Warner, 'The past and future of the intelligence cycle, in *Understanding the intelligence cycle,* edited by Mark Phythian, (London, Routledge, 2013), p. 9.
[5] Johnson, L. K. *National security intelligence: secret operations in defense of the democracies,* (Cambridge, Polity, 2012), p. 8
[6] Jervis, R. *Why intelligence fails: lessons from the Iranian Revolution and the Iraq War,* (Ithaca, Cornell University Press, 2010), p. 2-3.

policymakers cannot ignore information which they do not have, which is why effective intelligence collection is a vital step in the intelligence cycle. Espionage is one the oldest forms of such collection, a term that has traditionally been associated with both *spying*, and the recruitment and handling of those who become *spies* (or 'agents').[7] But over time, espionage has acquired what Demarest describes as ample 'pejorative baggage', often being conflated with methods of collection more technical, rather than human, in nature.[8] For example, the CIA's former Inspector General, Frederick Hitz, argues that espionage is defined by to its 'clandestinity' and "illegal means", a distinction so broad that it incorporates everything from overflights to outright theft.[9] Alternatively, it is more often pigeonholed under the banner of 'human intelligence' (HUMINT), a term that also incorporates many forms of collection beyond the classic conception of a spy, as Johnson demonstrates:

> Sometimes the phrase "humint" refers narrowly to the use of agents by intelligence professionals for the clandestine acquisition of documents or other secrets; more recently, its usage has expanded to incorporate all information collection by human beings, whether gathered overtly or covertly, and whether the instruments of collection are individuals in the diplomatic corps, the military, the intelligence agencies, or non-governmental personnel under temporary contract to the government ("outsourced" human intelligence).[10]

These distinctions are so broad as to be unhelpful, hence this thesis builds upon conventional conceptions by proposing that espionage is both the act, and process, of *clandestinely* acquiring human *agents* who *maintain* authorised access to classified information. With this emphasis on agents, espionage is immediately distinguished from technical intelligence, since the human source is ultimately responsible for the

[7] Scott, L. 'Human intelligence' in *Routledge Companion to Intelligence Studies*, edited by Robert Dover, Michael S. Goodman, and Claudia Hillebrand (Abingdon, Routledge, 2014), p. 96
[8] Demarest, G. B. 'Espionage in international law', *Denver journal of international law and policy,* 24:2, 1996, p. 324
[9] Hitz, F. P. *Why spy? Espionage in an age of uncertainty,* [Kindle version] (New York, St. Martin's Press, 2011). Accessed 24 September 2020, p. 17.
[10] Johnson, L. 'Evaluating "HUMINT": the role of foreign agents in U.S. security', *Comparative Strategy,* 29:4, 2010, p. 308-312

acquisition of secrets. Espionage is also distinct from the wider remit of human intelligence, since not all human sources operate from within the target state or organisation, nor are they necessarily facilitated by clandestine means. Diplomatic gossip, as a case in point, is most certainly HUMINT, but it is not espionage. Moreover, in comparison to defectors or prisoner interrogations, agents remain operationally active, offering an evolving source of intelligence.

Those responsible for recruiting and handling agents are employees of their respective intelligence organisations, known as intelligence officers (also referred to as 'operatives' in this study). Espionage, as such, is not about intelligence officers directly stealing secrets, but rather about 'recruiting others to do the dirty work'.[11] Those 'others' are sometimes referred to as *assets* in CIA parlance, however this is a confusing label since the agency also uses 'asset' to refer to sources who offer supporting services.[12] One particularly important form of asset is the principal agent, a person who is not an official member of any intelligence organisation but acts as 'spotter' or even a handler for agents.[13] It is also of note that since the early Cold War, agents are usually compartmentalised, meaning they do not recruit sources of their own. While spy networks were, for a time, highly common, the compromise of one source often led to the compromise of others, steering Western agencies towards a linear model, with the agent as the endpoint.[14]

In its simplest conception, *tradecraft* is the 'particular methods an intelligence officer uses to operate and communicate with sources without being detected by the

[11] Lucas, E. *Deception*, p. 125
[12] Scott, L. 'Human intelligence', p. 96; Mahle, M. B. *Denial and deception: an insider's view of the CIA* (New York, Public affairs, 2005), see Glossary of intelligence and national security terms.
[13] Former CIA officer, Miles Copeland, made this claim in 1975, but this author can find no evidence to suggest this trend has changed. For more details, see Copeland, M. *The real spy world* (London, Weidenfeld & Nicolson, 1975), p. 113.
[14] Ibid.

opposing intelligence service'.[15] These methods are necessary for agents to be acquired and managed, through a process commonly known as the 'agent acquisition cycle'.[16] And while tradecraft is often associated with covert communications, in fact it is more of a 'catch all' term, entailing a range of activities necessary for operational success.[17] But to fulfil its purpose, tradecraft must remain undetectable to *counterintelligence*, an all-encompassing term that pertains to the agencies and methods of defensive forces.[18] There are various definitions of counterintelligence dependent on the context to which it is implied, but the simplest and most suitable conception is offered by William R. Johnson, that counterintelligence is "aimed against intelligence, against active, hostile intelligence, against enemy spies".[19] Counterintelligence encompasses a wide umbrella of threats, including protective security, deception, investigations to uncover spies (often misleadingly dubbed "counterespionage"), and offensive actions against opposing intelligence agencies.[20] It is, therefore, a threat that permeates espionage, from the visible presence of surveillance teams on the streets of foreign cities, and the locked vaults of classified archives, to more insidious dangers such as 'moles' inside the ranks of intelligence agencies.[21] Consequently, a 'hard target' can be best defined as a state or non-state actor whose counterintelligence substantially raises the costs and risks for intelligence collection by the opposing side.

---

[15] Shulsky, A. N. & Schmitt, G. J. *Silent warfare: understanding the world of intelligence,* (Washington, Brassey's, 2002), p. 19.
[16] Lowenthal, M. *Intelligence: From secrets to policy,* [Kindle version], (Thousand Oaks, CQ Press, 2017). Accessed 1 March 2018, p. 137.
[17] Hitz, F. P. *The great game: the myths and reality of espionage,* [Kindle version] (New York, Vintage, 2005). Accessed 20 December 2020, p. 66.
[18] Ehrman, J. 'What are we talking about when we talk about counterintelligence?', *Studies in Intelligence, CIA,* 53:2, 2009, p. 15-17; Van Cleave, M. 'Strategic counterintelligence: what is it and what should we do about it?' *Studies in Intelligence,* 51:2, 2006, pp. 1-22.
[19] Prunckun H. *Counterintelligence theory and practice* [Google Play Books] (Lanham, MD, Rowman & Littlefield Publishers, 2012). Accessed 11 January 2018, p. 38.
[20] Ehrman, J. 'What are we talking', p. 5-18.
[21] Ibid.

In the United Kingdom, responsibility for espionage falls under the Secret Intelligence Service (SIS), informally known as MI6.[22] Headquartered in Vauxhall Cross, SIS remains an autonomous, civilian agency, whose very existence was only publicly acknowledged in 1994.[23] In the United States, chief responsibility for espionage belongs to the Central Intelligence Agency (CIA), an autonomous agency founded in 1947 and headquartered in Langley.[24] Although similar to SIS in its HUMINT prerogative, the CIA also undertakes a wider array of activities, including open-source collection, satellite and drone programmes, and all-source analysis.[25] Within this morass, the Directorate of Operations (DO), formerly known as the National Clandestine Service, takes the helm of espionage and covert action.[26] As the two agencies primarily responsible for British / American espionage, SIS and the CIA constitute the focus of this study. However, both exist within two diverse security communities. In the UK, alongside the Defence Intelligence agency (DI), and the Joint Terrorism Analysis Centre (JTAC), SIS's sister agencies include the Security Service (MI5) and Government Communication Headquarters (GCHQ). MI5 leads in domestic security, with a distinctly counterintelligence and counterterrorism focus, while GCHQ holds responsibility for domestic and foreign technical intelligence.[27] With their mandate for foreign spying, both SIS and GCHQ report to the Foreign Secretary, and

[22] SIS – Our history. Available at: https://www.sis.gov.uk/our-history.html [accessed 1 March 2018].
[23] Jeffrey, K. *MI6: the history of the Secret Intelligence Service 1909-1949* (London, Bloomsbury, 2011), p. 599-602.
[24] Andrew, C. *For the President's eyes only: secret intelligence and the American presidency from Washington to Bush*, (New York, HarperPerennial, 1996), p. 168-69; Zegart, A. *Flawed by design: the evolution of the CIA, JCS, and NSC*, (Stanford, Stanford University Press, 1999), p. 180-184; CIA - History of the CIA. Available at: https://www.cia.gov/about-cia/history-of-the-cia [accessed 1 March 2018].
[25] Riley, P. R. 'CIA and its discontents', in *Intelligence and National Security: The Secret World of Spies*, edited by Loch K. Johnson & James J. Wirtz, (Oxford, Oxford University Press, 2008), p. 56.
[26] CIA – Directorate of Operations (formerly known as the Clandestine Service). Available at: https://www.cia.gov/careers/opportunities/clandestine/index.html [accessed 1 March 2018].
[27] Cabinet Office (19 November 2010) National Intelligence Machinery. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61808/nim-november2010.pdf p.8 [accessed 1 March 2018], p.8-10.

are accountable to the Parliamentary Intelligence and Security Committee.[28] Conversely, the CIA exists within a nebula of 17 intelligence and security agencies, under the wider umbrella of the Director of National Intelligence (DNI).[29] Most prominent of these are the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA), performing similar functions to MI5 and GCHQ respectively.[30] Oversight of this enormous intelligence community is held by the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence, with the DNI reporting to the President.[31] Hence, while SIS and CIA are autonomous agencies with mandates for foreign espionage, they operate within a wider, democratically accountable intelligence apparatus.

Key cyber concepts

Most official definitions prescribe cyberspace to the confluence and interconnectivity of networks, hardware, and software that have emerged through the information revolution. For example, the British definition, provided by the *Centre for the Protection of National Infrastructure,* describes cyberspace as 'the term used to describe the electronic medium of digital networks used to store, modify, and communicate information. It includes the Internet but also other information systems that support businesses, infrastructure and services.'[32] The US *Department of Homeland Security* presents an equally broad view, defining cyberspace as the

[28] Ibid, p. 27-28.
[29] Office of the Director of National Intelligence – What we do. Available at: https://www.dni.gov/index.php/what-we-do [accessed 1 March 2018].
[30] Office of the Director of National Intelligence – Members of the IC. Available at: https://www.dni.gov/index.php/what-we-do/members-of-the-ic [accessed 1 March 2018].
[31] Belfer Center (July 2009) Congressional oversight of the Intelligence community. Available at: https://www.belfercenter.org/publication/congressional-oversight-intelligence-community [accessed 1 March 2018].
[32] CPNI – National security threats: cyber. Available at: https://www.cpni.gov.uk/cyber [accessed 1 December 2018].

'interdependent network of information technology infrastructures, that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers'.[33] These view cyberspace as greater than the World Wide Web or the Internet, and substantially differ from its original conception by William F. Gibson, where 'cyberspace' referred to a fictional, virtual, interactive environment, shaped by billions of operators.[34] As Betz and Stevens argue:

> The term is widely used as an equivalent of the Internet or the World Wide Web; and generally in the public consciousness it is seen as a very new thing, seemingly coming from nowhere and exploding into ubiquity within a couple of decades.
>
> However, cyberspace is not to be confused with the Internet. The former is a metaphor, while the latter is composed of real hardware: a global network of computers using standard protocols to communicate with one another. Nor is it the same thing as the World Wide Web, the system of interlinked, hypertext documents that are accessed via the Internet.
>
> Moreover, cyber is not all that new. We associate it with computer technology that has only relatively recently entered our homes; but in actuality it is a hybrid of telephones, television and computers, each with its own history and characteristics, which are in the process of converging.[35]

Scholars, however, contend that any workable definition must account for this human interactivity, which is seen as a core component for cyberspace's very existence. [36] As is argued by Ottis and Lorents' cyberspace 'is an artificial space, created by humans for human purposes. Without human users cyberspace would stagnate, fall into disrepair and eventually - cease to be.'[37] Furthermore, it is time-dependent, as opposed to static, constantly evolving pursuant to how humans interact with it, or how technological advances shape that interaction, 'dramatic changes can take place in extremely short

[33] Department of Homeland Security – Explore terms: a glossary of common cybersecurity terminology. Available at: https://niccs.us-cert.gov/about-niccs/glossary [accessed 1 December 2018].
[34] Ottis, R., Lorents, P. 'Cyberspace: definition and implications.' *Proceedings of the 5th International Conference on Information Warfare and Security*, 2010, p, p. 267.
[35] Betz, J. D. & Stevens, T. *Cyberspace and the state: toward a strategy for cyber power* [Kindle version] (Abingdon, Routledge 2011). Accessed 30 January 2017, see Introduction.
[36] Ottis, R., Lorents, P. 'Cyberspace: definition and implications', p. 268-9.
[37] Ibid.

time in cyberspace.'[38] Due to this aspect of change, it is generally easier to determine what cyberspace *isn't* rather than what it *is.*[39] As Klimburg argues, since governments, businesses and citizens generally 'know intuitively that cyberspace is the sum of all existing and future uses of the Internet by humans', its definitions 'are constantly changing'.[40] Thus, while cyberspace can be considered something of a 'metaphor' for a space facilitated by the Internet and the World Wide Web, it is more ethereal in meaning.[41] It is arguably the sum of modern computing, its interconnectivity, and the subsequent human interactivity that these convergences enable.[42] Simply put, it is, as Klimburg adds, the "world behind your screen":

> Cyberspace includes the vast number of private internets, many of them separated ("air-gapped," in the lingo) from the Internet per se, but nonetheless reachable through the use of thumb drives or other portable media. Your supermodern kitchen fridge, if it is in any way connectable to the Internet, is a part of cyberspace, as is your car, your phone, the data stored on your USB stick, your bank records, or your gym membership account. Anything you do or say or try to affect through internet technology—ranging from declaring your love via Facebook to planning a trip to looking up the weather—is part of cyberspace.[43]

Therefore, this thesis adopts the definition provided by Ottis and Lorrents, that cyberspace is 'a time-dependent set of interconnected information systems and the human users that interact with these systems'.[44] It is, as Warner adds, the 'impetus of the digital revolution', and has carried significant consequences for states, societies, and their intelligence and military affairs: '[every] government and intelligence system is feeling the effects of the digital revolution. Concepts, organizations, and doctrines that intelligence systems had created and maintained during the analog revolution of the

[38] Ibid, p. 269.
[39] Klimburg, A. *The darkening web: the war for cyberspace,* [Kindle version] (New York, Penguin Books 2018). Accessed 30 January 2018, p. 26.
[40] Ibid.
[41] Betz, J. D. & Stevens, T. *Cyberspace and the state,* see Introduction
[42] Klimburg, A. *The darkening web,* p. 26.
[43] Ibid.
[44] Ottis, R., Lorents, P. 'Cyberspace: definition and implications', p. 268.

twentieth century now have to be revised'. [45] Evidence to this effect became clear in 2004, when the Pentagon declared cyberspace to be a new domain for military action alongside land, air, and sea.[46] As of this decision, cyberspace ceased to be seen as a simple confluence of technologies, and became a new battlespace, to be fought by an entirely different kind of soldier to those of the past.

Whether or not cyberspace should actually constitute a new domain for warfare has been hotly debated, but the fact remains that it is has enabled new means to exert intelligence and military action.[47] The impact of cyberspace on warfighting can be seen in two key respects, with the first pertaining to the evolution of physical force manifested through so-called network centric warfare.[48] As is often discussed through RMA literature (revolution in military affairs), cyberspace is seen as a conduit to enhance the speed, precision, and efficiency of conventional force.[49] Second, the threat posed from infecting critical infrastructure or military hardware with detrimental viruses has coalesced into various debates about the nature of, and rules of governance for, 'cyber warfare'.[50] In effect, cyberspace is now regarded as a domain for the actual expression of force, where physical and electronic harm can be exerted through digital means.[51] This is illustrated by the elevation of US Cyber Command, created in 2008, to a unified command under STRATCOM, meaning it reports directly to the Secretary of

[45] Warner, M. 'Reflections on technology and intelligence systems' *Intelligence and National Security,* 27:1, 2012, p. 144.
[46] Ibid, p. 150.
[47] U.S. Cyber Command - U.S. Cyber Command History. Available at: https://www.cybercom.mil/About/History/ [accessed 23 May 2020].
[48] Betz, J. D. & Stevens, T. *Cyberspace and the state,* see chapter 3; Ferris, J. 'Netcentric warfare, C4ISR and information operations: towards a revolution in military intelligence?', in *Understanding Intelligence in the Twenty-First Century, edited by L. V. Scott and P. D. Jacking',* (London, Routledge, 2004), p. 54.
[49] Ibid.
[50] Stinissen, J. 'A legal framework for the cyber operations in Ukraine', in *Cyber War in Perspective: Russian Aggression Against Ukraine,* edited by Kenneth Geers, (Tallinn, NATO CCD COE, 2015), p. 123-134.
[51] Rid, T. *Cyber war will not take place,* (Oxford, Oxford University Press, 2013), p. 3.

Defense.[52] As the US Cyber Command website notes, this 'was seen as a recognition of the growing centrality of cyberspace to U.S. national security and an acknowledgement of the changing nature of warfare'.[53] Some views posit that cyberspace has also lowered the barriers of entry to conflict for state and non-state actors alike, potentially changing not just the methods of warfare but also its participants.[54] Armed with an Internet connection and a skillset, modern combatants do not necessarily need soldiers, navies, and air forces to engage in military action, nor is their outreach stymied by the geographical limitations of conventional force. However traditionalists such as Rid and McBurney reject this view, who contend that even in cyberspace, complex operations that would yield effective gains against well-defended states, are likely to be available only to a handful of nation-state actors.[55]

Cyberspace has also led to profound revisions of intelligence, particularly through its influence upon open source, technical, and analytical specialisms.[56] For example, ever growing passive eavesdropping and the emergence of non-invasive forms of collection such as 'social media intelligence' (SOCMINT) are considered to be shifting burdens from collection towards analysis, meaning it is often easier to acquire information, but also more resource intensive to turn this deluge of data into actionable intelligence.[57] It has also led to an entirely new form of intelligence gathering entitled 'cyber espionage', which in its narrowest sense is considered the theft

[52] U.S. Department of Defense (18 August 2017) DoD initiates process to elevate U.S. Cyber Command to unified combatant command. Available at: https://www.defense.gov/Explore/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/ [accessed 34 May 2020].
[53] Oakley, J. G. *Waging cyber war: technical challenges and operational constraints*, (Berkeley, Apress, 2019), p. 2.
[54] Langlo, H-I. 'Competing academic approaches to cyber security', in *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*, edited by Karsten Friis and Jens Ringmose, (London, Routledge, 2016), p. 14.
[55] Ibid.
[56] Warner, M. 'Reflections on technology and intelligence systems', p. 143-150.
[57] Omand, D., Bartlett, J., Carl, M. 'Introducing social media intelligence (SOCMINT)', *Intelligence & National Security*, 27:6, 2012, p. 810-813.

of information through computer networks, by tools and techniques commonly known as 'hacking'.[58] It is distinct from espionage by its independence from human sources, insofar as that while hacking can be aided by human agents, it is not necessarily dependent upon them.[59] Akin to cyber warfare, cyber espionage is viewed as a force multiplier for heavily and lesser resourced actors alike, perceived to allow criminals, terrorists, and smaller nations to expand their intelligence outreach.[60] Once again, however, traditionalists reject this perspective, on the basis that those who value their secrets will naturally take steps to protect them, pushing up the burden of cost to the collector.[61] But although cyberspace has led to new disciplines and challenges for intelligence, it has not replaced classic espionage, which remains the focus of this study. That said, while it may be a leap to follow in the military's footsteps by heralding a new domain for spies, it is shown in the proceeding section that cyberspace poses profound opportunities for espionage.

Literature review: the optimists vs. pessimists

While technology's influence on the realms of warfare, intelligence and security, has attracted a vast array of analysis, its impact on espionage affairs remains largely the domain of science fiction more so than scholarship.[62] As personified through classics

[58] Rid, T. *Cyber war will not take place*, p. 81-83.
[59] Ibid,
[60] Warner, M. 'Reflections on technology and intelligence systems', p. 148; Clarke, R. A. & Knake, R. K. *Cyber war: the next threat to national security and what to do about it,* [Kindle version] (New York, HarperCollins, 2010). Accessed 23 March 2020, p. 232.
[61] Rid, T. *Cyber war will not take place*, p. 81-83.
[62] For a snapshot of contemporary literature, see: Aldrich, R. J. *GCHQ: the uncensored story of Britain's most secret intelligence agency* [Kindle version] (London, HarperPress, 2010). Accessed 12 March 2019; Corera, G. *Intercept: the secret history of computers and spies,* [Kindle version] (London, Weidenfeld & Nicolson, 2015). Accessed 21 November 2020; Greenwald, G. *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state,* (New York, Metropolitan Books, 2014); Edgard, T. H. *Beyond Snowden: privacy, mass surveillance, and the struggle to reform the NSA*, (La Vergne, Brookings Institution Press, 2017); Schneier, B. *Data and Goliath: the hidden battles to collect your data and control your world,* [Kindle version] (New York, W. W. Norton & Company, 2015). Accessed 1 March 2019; Landau, S. 'Making sense from Snowden: what's significant in the NSA surveillance revelations', *IEEE Security & Privacy,* 11:4, 2013); Verble, J. 'The NSA and Edward Snowden: surveillance in the

such as James Bond and The Man from U.N.C.L.E, spy gadgets have long captured public imaginations.[63] In the Cold War, Langley's gadget laboratory, *The Office of Technical Services* (OTS), even briefly reassigned technicians 'to telephone duty' following each new episode of *Mission: Impossible*, to placate overexcited intelligence officers asking "Could OTS do *that?*".[64] But the public's fascination for spy gadgets has not been reflected in academia, a factor that is unsurprising given, as Quinlan contends, that tradecraft (broadly speaking) 'is commonly regarded as either scholarly antiquarianism or the stuff of movies. Almost no academic book on international relations considers it'.[65] This is partially explained by the negative connotations often associated with the study of intelligence's operational affairs and bureaucratic structures.[66] Richard Aldrich prescribes well-documented early studies into the 'minutiae' of intelligence work to what he labels the "train-spotter school".[67] These authors, he claims, failed to convey the significance of their findings to the shaping of 'international events', leading to what Robert Winks 'succinctly' defines as the "So

21st Century', *ACM SIGCAS Computers and Society,* 44:3, 2014; Bamford, J. *The shadow factory: the Ultra-Secret NSA from 9/11 to the eavesdropping on America* [Kindle version] (New York, DoubleDay, 2008); Benes, L. 'OSINT, new technologies, education: expanding opportunities and threats. A new paradigm', *Journal of Strategic Security,* 6:3, 2013; Omand, D. Bartlett, J. Miller, C. 'Introducing social media intelligence (SOCMINT)*';* Ivan, A. L. et al. 'Social media intelligence: opportunities and limitations', *CES Working Papers,* 7:2, 2015; Omand, D. 'Social media intelligence (SOCMINT)', *The Palgrave Handbook of Security, Risk, and Intelligence*, (London, Palgrave Macmillan, 2017); Valeriano, B. & Maness, R. C. *Cyber war versus cyber realities: cyber conflict in the international system,* (Oxford, Oxford University Press, 2015); Sharma, A. 'Cyber wars: a paradigm shift from means to end', *The Virtual Battlefield: Perspectives on Cyber Warfare,* edited by Christian Czosseck & Kenneth Geers (Amsterdam, IOS Press, 2009); Berkowitz, B. *The new face of war: how war will be fought in the 21st century* (New York, The Free Press, 2003); Libicki, M. C. *Conquest in cyberspace: national security and information warfare,* (Cambridge, Cambridge University Press, 2010); Cordesman, J. G. *Cyber-threats, information warfare, and critical infrastructure protection: defending the U.S. homeland,* (Westport, Praeger, 2002); Warner, M. *The rise and fall of intelligence: an international security history,* [Kindle version] (Washington, Georgetown University Press, 2014).. Accessed 12 January 2021.

[63] Hitz, F. P. *The great game*, p 128.

[64] Wallace, R. et al. *Spycraft: inside the CIA's top secret spy lab,* (London, Bantam Press, 2008), p. 112.

[65] Quinlan, K. *The secret war between the wars: MI5 in the 1920s and 1930s* (Rochester, NY, The Boydell Press, 2014), p. xviii.

[66] Aldrich, J. R. 'Intelligence, Anglo-American Relations and the Suez Crisis, 1956', *Intelligence and National Security,* 9:3, 2008, p. 544.

[67] Ibid.

what?" question.[68] As such, from the 1980s onwards, interest in operational minutia gave way to more impactful queries about intelligence in world affairs, mostly leaving tradecraft (and spy gadgets) to the realm of fiction.[69]

This disregard for the 'minutiae' of intelligence work is unjust, considering the 'methods used by spies' have enabled intelligence in support of 'many of the major foreign policy initiatives of the twentieth and twenty-first centuries'.[70] The study of tradecraft does not detract from intelligence's significance to international relations, rather, it allows scholars to understand how wider events transpire: 'ignoring HUMINT tradecraft would be equivalent to ignoring military hardware; just as the military relies on arms, so agent operations rely on tradecraft'.[71] However, from a historical perspective, tradecraft has seen renewed interest in recent years, owing to a small but thoroughly detailed body of work focused specifically on the innovations developed throughout the mid-late Cold War.[72] One of these works, *Spycraft* (2008), co-authored by the former chief of Langley's tradecraft laboratory, Robert Wallace, alongside Keith Melton and Henry Schlesinger, ended with a brief consideration about how cyberspace and digital technology might affect modern espionage.[73] The findings of Wallace et al, despite being somewhat outdated, only considered the opportunistic benefits of modern technology, without seriously weighing its operational limitations.[74] This reflects a trend that has been continued by later (and generally less developed) works, whereby

[68] Ibid.
[69] Ibid.
[70] Quinlan, K. *The secret war between the wars*, p. xviii
[71] Ibid.
[72] For key examples, see: Wallace, R. et al. *Spycraft*; Mendez, A. et al. *The Moscow rules: the secret CIA tactics that helped America win the Cold War*, (New York, Public Affairs, 2019); Macrakis, K. *Seduced by secrets: inside the Stasi's spy-tech world*, [Kindle version] (Cambridge, Cambridge University Press, 2008).
[73] Wallace, R. et al. *Spycraft*, p. 443-460.
[74] Ibid.

cyber-enabled tradecraft is confined to brief, underdeveloped assumptions, which are lacking in critical analysis or hard-target considerations.[75]

But within this literature, it is commonly assumed that cyberspace carries game-changing benefits to espionage. One of the earliest and arguably most profound propositions is that spies might be recruited and handled *entirely* online, sidestepping the dangers of personal meetings.[76] Wallace argues that through secure communications backed by video link, intelligence officers could run "virtual personal meetings" with their agents.[77] He illustrates that point with the example of Robert Hanssen, a former Soviet spy working within the FBI, who never once met his handlers.[78] However cases such as Hanssen's should be considered within a single digit minority, not least because as argued by the former deputy director of SIS, Nigel Inkster, in *Intelligence agencies in the Cyber World*, the absence of meetings 'raises substantial challenges in respect of establishing bona fides'[79] Former CIA case officer, David Gioe, builds upon this argument in *The More Things Change*, writing:

> Despite the advantages of technology, there is no substitute for the personal interaction between a case officer and his or her agent. Any case officer would want the 'gut-check' of meeting an agent personally in order to make a more comprehensive assessment of his or her suitability. The case officer would want

[75] Inkster, N. 'Intelligence agencies and the cyber world', *Strategic Survey*, (2012), p. 40; Brenner, J. *America the vulnerable: inside the new threat matrix of digital espionage, crime, and warfare* (New York, The Penguin Press, 2011), p. 167; Sano, J. 'The changing shape of HUMINT', *Intelligencer,* 21:3, 2015, p. 78-79; Lucas, E. *Spycraft rebooted: how technology is changing espionage,* [Kindle version], (Seattle, Amazon Publishing, 2018). Accessed 5 January 2019, see chapters 2 & 6; Grey, S. *The new spymasters: inside espionage from the Cold War to global terror,* (New York, Viking, 2015), p. 271-274; Gosler, J. R. 'The digital dimension', in *Transforming U.S. Intelligence, edited by Jennifer E. Sims & Burton Gerber,* (Washington, Georgetown University Press, 2005), p. 96-100; Tucker, D. *End of intelligence: Espionage and state power in the information age,* (Palo Alto, Stanford University Press, 2014), p. 56; Gioe, D. V. 'The more things change': HUMINT in the cyber age', in *The Palgrave Handbook of Security, Risk and Intelligence,* edited by Robert Dover, Huw Dylan, and Michael Goodman (London, Palgrave, Macmillan, 2017); Wallace, R. 'A time for counterespionage', in *Vaults, Mirrors, & Masks: Rediscovering U.S. Counterintelligence,* (Washington, Georgetown University Press, 2008); Tal, A. & Siman-Tov, D. 'HUMINT in the cybernetic era: gaming in two worlds', *Military and Strategic Affairs,* 7:3, 2015.

[76] Inkster, N. 'Intelligence agencies and the cyber world', p. 40.

[77] Wallace, R. 'A time for counterespionage', p. 114.

[78] Ibid, p. 110.

[79] Inkster, N. 'Intelligence agencies and the cyber world', p. 40; Gioe, D. V. 'The more things change', p. 225.

> to hear, in person, why his agent decided to take the risk to work for a foreign intelligence service'.[80]

For Gioe, the interpersonal meeting is not simply a matter of trust, but of supporting agents in times of personal and emotional crisis:

> A good deal of any human communication is done through non-verbal means, and part of HUMINT is interpreting unspoken communication such as mood and body language … A touch on the arm, or a look in the eye, a calming act of kindness, a well-timed, thoughtful gift, and some reassuring words of encouragement are all necessary parts of running a human agent.[81]

There is a strong basis for Gioe's claims. Studies such as Nicholas Wheeler's *Trusting Enemies,* have shown that interpersonal trust only rises in importance within high stakes situations, such as when navigating the security dilemma.[82] Moreover, psychologists have often shown that online human connections, even those by video link, are not as fully engaging as a face-to-face encounter, despite the fact that low-level trust often develops faster in cyberspace than in person.[83] As Hegghammer argues in *Interpersonal trust on Jihadi internet forums,* 'when stakes of an interaction increase to involve … the love, money, or especially the personal safety of the truster, then it

---

[80] Gioe, D. V. 'The more things change', p. 221-222.
[81] Ibid.
[82] Wheeler, N. J. *Trusting enemies,* [Kinde version] (Oxford, Oxford University Press, 2018). Accessed 17 January 2021, p. 1-2.
[83] For examples, see: Lawson, H. M. & Leck, K. 'Dynamics of Internet dating', *Social Science Computer Review,* 24:2, 2006, p. 199-205; Madianou, M. & Miller, D. 'Polymedia: towards a new theory of digital media in interpersonal communication', *International Journal of Cultural Studies,* 16:2, 2012, p. 170-173; Sherman, L. E., Michikyan, M. & Greenfield, P. M. 'The effects of text, audio, video, and in-person communication on bonding between friends', *CyberPsychology,* 7:2, 2013, p. 2-10; Ben-Ze'ev, A. 'Privacy, emotional closeness, and openness in cyberspace', *Computers in Human Behaviour,* 19:4, 2003, p. 466; McKenna, K. Y. A., Green, A. S. & Gleason, M. E. J. 'Relationship formation on the Internet: what's the big attraction?', *Journal of Social Issues,* 58:1, 2002, p. 30; Hegghammer, T. 'Interpersonal trust on Jihadi internet forums', *Norwegian Defence Research Establishment,* 2014, p. 7-8; Nitsch, H. & Irani, D. 'Prevention, anti-radicalisation and the role of social media: a view from Germany', in *Terrorists' use of the Internet: Assessment and Response*, edited by Maura Conway, Lee Jarvis, Orla Lehane, Stuart Macdonald, & Lella Nouri (Amsterdam, IOS Press, 2016), p. 260-264; Jones, H. S. & Towse, J. 'Examinations of email fraud susceptibility: perspectives from academic research and industry practice', in *Psychological and Behavioral Examinations in Cyber Security,* (Hershey, IGI Global, 2018), p. 90-91; Cialdini, R. B. & Guadagno, R. E. 'Online persuasion and compliance: social influence on the Internet and beyond, in *The Social Net: The Social Psychology of the Internet*, edited by Y. Amichai-Hamburger, (Oxford, Oxford University Press, 2009), p, 104; Silva, E. D. 'Detecting individual-level deception in the digital age: The DETECT model', in *National security and counterintelligence in the era of cyber espionage*, edited by Eugenie de Silva (Hershey, Information Science Reference, 2016), p. 269; Ryan, T. "Getting in bed with Robin Sage", *BlackHat USA,* 2010, p. 2.

becomes a different ballgame.'[84] For example, non-verbal cues are often distorted through text and video mediums, leading to an experience that is more awkward and less interpersonally expressive.[85] These arguments reinforce Gioe's point, and steer away from the notion of a solely online relationship.

That said, most of the literature presents cyberspace not as a replacement for personal meetings, but as an aid, reducing dependency on the interpersonal dimension by empowering four crucial functions of tradecraft. The first of these functions is *recruitment*, the process by which agents are acquired. Traditionally, spies were either recruited through face-to-face rapport building or volunteered by approaching foreign officials, both of which were aided to a limited extent by social communications such as letters and telephones.[86] But Tal and Siman-Tov, in *HUMINT in the cybernetic era*, argue that today's intelligence officers can use fake online identities to recruit prospective spies through Internet forums and online social channels.[87] They argue that messages can 'vanish into the vast sea of information', burying social communications within an ever growing avalanche of data.[88] These proposals are not, however, without merit, since as CIA psychologist Ursula Wilder adds in *The Psychology of Espionage and Leaking in the Digital Era*, cyberspace's social benefits are ideal for radicalising vulnerable people into a range of malicious activities, including crime, terrorism, and espionage.[89] As illustrated by Lucas in *Spycraft Rebooted*, even online video games, a popular form of social bonding, could be used to cultivate foreign officials.[90]

---

[84] Hegghammer, T. 'Interpersonal trust on Jihadi internet forums', p. 7-8
[85] Silva, E. D. 'Detecting individual-level', p. 261-265; Sherman, L. E., Michikyan, M. & Greenfield, P. M. 'The effects of text, audio, video, and in-person communication on bonding between friends', p. 2-10.
[86] For key examples, see: Clarridge, D. R & Diehl, D. *A spy for all seasons: my life in the CIA*, [Kindle version] (New York, Scribner, 1997). Accessed 1 March 2018, chapter 7; Royden, B. G. 'Tolkachev, a worthy successor to Penkovsky', *Studies in Intelligence, CIA,* 47:3, 2008, p. 20.
[87] Tal, A. & Siman-Tov, D. 'HUMINT in the cybernetic era', p. 96.
[88] Ibid, p. 98.
[89] Wilder, U. M. 'The psychology of espionage and leaking in the digital era', *Studies in Intelligence, CIA*, 61:2, 2017, p. 6.
[90] Lucas, E. *Spycraft rebooted,* see chapter 6.

Recruiters, he claims, might use these social mediums to 'soften' up their sources, before requesting a personal meeting where the offer to spy is delivered face-to-face.[91] Alternatively, Althoff, in *Human Intelligence,* proposes that instead of recruiting spies directly, volunteers 'no longer have to take the dangerous step of walking into a foreign embassy or covertly expressing their interest in a note or personal aside to a case officer. They can simply send an e-mail to an intelligence service's website', thereby skipping lengthy cultivation processes altogether.[92]

The second function of tradecraft is *surveillance*, whereby personal information is gathered to spot and assess potential agents.[93] Traditionally, insights into a target's personal affairs and suitability for spy work were (beyond rapport building) gathered by covertly observing sources, or by planting technical listening devices inside embassies and apartments.[94] However vast amounts of information can be acquired through what Gioe describes as the 'twin cyber giants' of social media and hacking.[95] Social networks, for example, are generally awash with personal information, much of which individuals choose to share publicly, meaning lengthy periods of rapport building could be skipped with a cursory glance of Facebook. Hacking, by comparison, might offer a pathway to private information, given that enormous amounts of personal information are contained within databases, personal devices, and the cloud. A largescale breach of a major organisation, such as a government agency, could offer lists of persons with access to desired information, while the hacking of a target's smartphone or computer offers a window into their day-to-day affairs.[96]

[91] Ibid.
[92] Althoff, M. 'Human intelligence', in *The five disciplines of intelligence collection,* edited by Mark M. Lowenthal &Robert M. Clark (Thousand Oaks, CQ Press, 2016), p. 75.
[93] Gioe, D. V. 'The more things change', p. 219.
[94] Easter, D. 'Soviet Bloc and Western bugging of opponents' diplomatic premises during the early Cold War', *Intelligence and National Security,* 3:1, 2016, p, 31.
[95] Gioe, D. V. 'The more things change', p. 218; Lucas, E. *Spycraft rebooted,* see chapter 2.
[96] Ibid.

The third function is *handling*, wherein the intelligence officer must assess, support, and task their agent, as well as receive their intelligence. Traditionally, agents were handled through personal and impersonal covert communications, such as dead-drops and secret writing, but the advent of encrypted email opened the prospect of handling by cyber means.[97] According to Wallace et al, by the early millennium intelligence agencies were already adopting strong commercial encryption, including off-the-shelf systems such as *Pretty Good Privacy* (PGP), to send covert messages to their agents.[98] But later developments are seen to have advance these prospects, with Gioe describing tools such as The Onion Router, which anonymises Internet traffic and facilitates access to the 'dark web', as something of a 'a tradecraft revolution'.[99] Consequently, today's agents could theoretically be handled in real-time, transmitting intelligence at their own convenience, as Inkster argues, 'from a practical perspective, the increasingly pervasive nature of ICT looks likely to reduce a long-standing problem faced by intelligence agencies of agents with good access but unable to report their intelligence in a timely manner'.[100] These are, again, reasonable assumption, since such developments have placed serious strains on law enforcement and technical intelligence agencies.[101] As Aldrich adds in *GCHQ*, encrypted online communications have 'favoured the code-makers', while pushing the 'code-breakers firmly into second place'.[102] Thus, while operatives will still need to meet their agents, at least from time

[97] For more details: Wallace, R. et al. *Spycraft*, p, 115-116 & 393; Weiser, B. *A secret life: the Polish officer, his covert mission, and the price he paid to save his country*, [Kindle version] (New York, Perseus, 2004). Accessed 24 July 2020, see chapter 3; Mendez, A. et al. *The Moscow rules*, p. 85; Everett, J. A. *The making and breaking of an American spy,* (Durham CT, Strategic Book Group, 2011), p. 65-66.
[98] Wallace, R. et al. *Spycraft,* p. 451-452.
[99] Gioe, D. V. 'The more things change', p. 220.
[100] Inkster, N. 'Intelligence agencies and the cyber world', p. 40.
[101] Bartlett, J. *The dark net: inside the digital underworld*, (London, William Heinemann, 2014), see chapter 3; Corera, G. *Intercept*, p. 270 & 353.
[102] Aldrich, R. J. *GCHQ*, p. 492.

to time, it seems increasingly possible that many aspects of handling, including tasking and direction, can be relegated to 'digital means'.[103]

The fourth and final function is *collection*, where the agent must actually exfiltrate the information they've been tasked to acquire. Conventionally, agents either took notes, or photographed documents with commercial or subminiature spy-cameras.[104] But according to the former director of the CIA's Clandestine Information Technology Office (CITO), James Gosler, in *The Digital Dimension,* the shift from paper-based to electronic storage carries profound revisions for collection, relegating photography to a 'minor role'.[105] In theory, agents could exfiltrate 'millions' of documents using little more than a 'microelectronic memory device'.[106] As Tal and Siman-Tov add, a simple USB thumb drive may be enough to transfer 'large amounts of multimedia information'.[107] Brenner however, questions whether the contemporary agent even needs to steal information themselves, 'perhaps your spy's job is no longer stealing information but planting malicious software from the inside to enable a remote cyberthief to snatch information later.'[108] In essence, the agent becomes an access point, uploading cyber tools that gather and transmit data back to intelligence agencies on their behalf.[109] There are certainly foundations for these claims, such as the Stuxnet virus, which devastated Iran's Natanz nuclear centrifuges and was potentially uploaded by a 'secret agent' with access to the plant's systems.[110]

The picture painted so far is notably optimistic (in terms of the benefits cyber-enabled tradecraft can bring), but what remains to be seen is how far these prospects

[103] Gioe, D. V. 'The more things change', p. 221.
[104] For more details: Wallace, R. et al. *Spycraft,* p. 89-90; Mendez, A. et al. *The Moscow rules,* p. 83; Royden, B. G. 'Tolkachev, a worthy successor to Penkovsky', p. 17.
[105] Gosler, J. R. 'The digital dimension', p. 96.
[106] Ibid.
[107] Tal, A. & Siman-Tov, D. 'HUMINT in the cybernetic era', p. 98.
[108] Brenner, J. *America the vulnerable,* p. 54.
[109] Ibid.
[110] Inkster, N. 'Intelligence agencies and the cyber world', p. 43.

can be carried into hard targets conditions. At least where communications are concerned, John Sano, the former deputy of the CIA's Directorate of Operations, is sceptical that cyberspace is a secure domain for espionage. In his 2015 paper *The Changing Shape of HUMINT,* Sano argues that '[while] crafting an approach via technical means … whether it's via e-mail or a social blog … might well be expeditious [it is] highly insecure'.[111] In Sano's view, while technology plays an 'important role in approaches and maintaining contact with an agent', its overreliance leaves espionage vulnerable to 'hostile counterintelligence activities', meaning such tools must be used in "moderation".[112] Similarly, Althoff argues that 'while recognizing the advantages of the Internet and social media', intelligence officers must 'also understand that these have inherent [counterintelligence] risks.'[113] David Tucker adds to these arguments in *End of Intelligence* (2014), contending that whatever 'their technical merits', modern tradecraft technologies are 'still used by humans, which inevitably injects error into the system'.[114] Tucker's remarks hints towards a deeper argument, by implying that human fallibilities are as significant an issue for tradecraft as counterintelligence threats.

Furthermore, these pessimistic views are only exacerbated by the well-documented history of Internet surveillance in Russia and China, which implies that cyberspace may be far less secure than often assumed.[115] As Ronald Deibert argues in

[111] Sano, J. 'The changing shape of HUMINT', 21:3, 2015, p. 79.
[112] Ibid.
[113] Althoff, M. 'Human intelligence', p. 75.
[114] Tucker, D. *The end of intelligence,* p. 76.
[115] For example, see: Deibert, R. J. *Black code: inside the battle for cyberspace,* (Toronto, McClellend & Stewart, 2013); Deibert, R. & Rohozinski, R. 'Beyond denial: introducing next-generation information access controls', in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace,* [Kindle version] (London, The MIT Press, 2010). Accessed 12 June 2020; Deibert, R. & Rohozinski, R. 'Control and subversion in Russian cyberspace', in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace,* [Kindle version] (London, the MIT Press, 2010). Accessed 12 June 2020; Soldatov, A. & Borogan, I. *The red web: the struggle between Russia's digital dictators and the new online revolutionaries,* [Kindle version] (New York, Public Affairs, 2015). Accessed 1 January 2018; Soldatov, A. & Borogan, I. (2013) 'Russia's surveillance state', World Policy journal. Available at: http://www.worldpolicy.org/journal/fall2013/Russia-surveillance [accessed 1 March 2018]; Inkster, N. 'The Chinese intelligence agencies: evolution and empowerment in cyberspace', in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai

Black Code (2013), contrary to idealistic notions that authoritarian regimes would 'wither in the face of the Internet', cyberspace has become 'just another excuse for state control'.[116] This is notably true for China, where the Internet was constructed with state surveillance front and centre.[117] Similarly, Russian investigative journalists Andrei Soldatov and Irene Borogan illustrate how Putin's regime, which initially took a restrained attitude to Internet surveillance, has recently followed China's oppressive model.[118] As they discuss in *The Red Web* (2015), the Kremlin views the Internet as a key vessel for political dissent, and has, in turn, expanded the legal and technical powers of its domestic security services.[119] At least, therefore, where communication is concerned, the value of cyberspace is open to doubt.

What these, and other emerging trends in security and counterintelligence mean for the prospects of hard-target espionage remain to be determined, but they infer that cyber-enabled tradecraft may be more complex than most of the literature indicates. Arguably, it would be naïve to assume that hard target states, eager to protect their own national interests, would not attempt to find weaknesses in their opponent's tradecraft, and yet this risk has been overlooked by intelligence scholars. However, Tucker's comments hit an all too important point, that whatever the technical merits of cyberspace, it is still used by human beings. This hints towards the notion that trust and behaviour play a much greater role in tradecraft than is portrayed by the optimistic camp, a factor that has not yet been fully considered.

Ming Cheung, & Reveron, D. S. (Oxford, Oxford University Press, 2015); Inkster, N. *China's Cyber Power*, [Kindle Version] (Abingdon, Routledge, 2016). Accessed 20 May 2017.
[116] Deibert, R. J. *Black code,* p. 18.
[117] Ibid, p. 62.
[118] Soldatov, A. & Borogan, I. *The red web*, see chapter 8.
[119] Ibid, see chapter 15.

Methodology: the merits of abduction

Reconciling these optimistic and pessimistic perspectives is no simple task, since espionage is a clandestine enterprise, meaning its current sources and methods remain classified. There is, for example, no public archive to review contemporary experiences, nor are practitioners likely forthcoming about their knowledge of cyber affairs. However, while the espionage world is secretive, the limitations of technology are not, and if intelligence officers want to operate in cyberspace, they must do so within its technical confines. This shifts the onus of research away from collecting evidence of classified capabilities, towards understanding how cyberspace's limitations relate to the realities of espionage. This, to a limited extent, is the approach adopted by the optimists, who considered cyberspace's perceived benefits in the context of tradecraft's various functions, summarised as follows:

1. Tradecraft is about recruitment; to identify and cultivate prospective spies and offer a path for volunteers
2. Tradecraft is about surveillance; to observe and understand prospective spies and accelerate the recruitment process.
3. Tradecraft is about handling; to manage and task those who spy and to receive their information.
4. Tradecraft is about collection; to enable spies to access and safely exfiltrate desired information.

The problem, therefore, is not with the method, but with its application, since it has not been sufficiently applied within the context of hard target conditions. That considered, given the significance of cyberspace to society at large, there is no shortfall of data pursuant to any of tradecraft's functions. For instance, The Onion Router, which is cited by Gioe as a potentially revolutionary tool for covert communications, purports around two million active daily users, and has been subjected to ample study by its own

developers, academics, and security specialists alike.[120] Likewise, while hacking may be useful for espionage purposes, a cursory search of *Google Scholar* for cybersecurity (a key hacking defence) returns over two hundred thousand results.[121] Herein lies the advantageous duality of cyberspace, since its impact on both defensive and offensive actors draws scrutiny from both perspectives. Texts such as Shavers and Bair's *Hiding behind the keyboard*, as a case in point, demonstrate the various methods law enforcement can use to detect covert communications and uncover anonymised online users.[122] While other texts, such as Kevin Mitnick's *The art of invisibility*, offer lessons and applied advice to those who wish to disappear in cyberspace.[123] In addition, rising public interest in the online activities of intelligence has seen an abundance of leaking and media attention. Edward Snowden, for example, released thousands of classified NSA documents (some of which is relevant to HUMINT) into the public domain, and through doing so his ability to plunder one of the world's most secure organisations has drawn ample questions by security pundits.[124] Similarly, China's penetration of the

[120] There are, for example, approximately 2,500 papers pertinent to Tor available in Google Scholar. Furthermore, its developers continue to publish research studies and emerging issues on Tor's home page, actively encouraging and integrating external research. For more details, see Tor – Directly connecting users, 2017-01-01 to 2018-01-01. Available at: https://metrics.torproject.org/userstats-relay-country.html?start=2017-01-01&end=2018-01-01&country=all&events=off [accessed 1 February 2018]; Tor Blog (22 July 2018) How to do effective and impactful research. Available at: https://blog.torproject.org/how-do-effective-and-impactful-tor-research [accessed 8 January 2019].
[121] For example, see Jang-Jaccard, J. 'A survey of emerging threats in cybersecurity', *Journal of Computer and System Sciences*, 80:5, 2014; Garfinkel, S. L. 'The cybersecurity risk', *Communications of the ACM*, 55:6, 2012; Buchanan, B. *The cybersecurity dilemma: hacking, trust, and fear between nations* (Oxford, Oxford University Press, 2016).
[122] Shavers, B. & Bair, J. *Hiding behind the keyboard: uncovering covert communication method with forensic analysis*, [Kindle version] (Cambridge MA, Syngress, 2016). Accessed 13 August 2017.
[123] Mitnick, K. D. & Vamosi, R. *The art of invisibility: the world's most famous hacker teaches you how to be safe in the age of big brother and big data* [Kindle version] (New York, Hachette Book Group, 2017). Accessed 20 December 2018.
[124] Snowden Archive – Welcome to the Snowden Digital Surveillance Archive. Available at: https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi [accessed 23 December 2020]; Business Insider (13 December 2013) NSA: Snowden stole 1.7 million classified documents and still has access to most of them. Available at: http://www.businessinsider.com/how-many-docs-did-snowden-take-2013-12?IR=T [accessed March 1 2018]; NBC News (26 August 2013) How Snowden did it. Available at: http://www.nbcnews.com/news/other/how-snowden-did-it-f8C11003160 [accessed March 1 2018]; Sanger, D. E. & Schmitt, E. (9 February 2014) Snowden used low-cost tool to best N.S.A, *The New York Times.* Available at: https://www.nytimes.com/2014/02/09/us/snowden-used-low-cost-tool-to-best-nsa.html?hp&_r=1 [accessed 23 July 2017].

Office of Personnel Management, one of the US government's most severe breaches, has led to both congressional and scholarly inquiries.[125] These, and other major events, including the release of thousands of CIA hacking documents by Wikileaks (dubbed Vault 7), and the disclosure of the CIA's online covert communications systems by Western press, helps paint a picture of cyberspace's potential benefits and limitations.[126] Consequently, the research challenge is not in acquiring new data, but in making sense of the data that already exists – what, therefore, is required is a means of developing guiding lessons, so as to better interpret the evidence.

Without a window into the secret world, it is necessary to turn to a form of reasoning commonly known as abduction.[127] Attributed to the works of Charles S. Pierce, abductive reasoning is the process of using established knowledge to better interpret new evidence.[128] In essence, it rests on the assumption of underlying rules, or causal mechanisms, that influence events even when they are not directly observable.[129] As Walton argues, the discovery of a knife on the window frame of a burgled house could lead to the conclusion that the knife had been used to pry open the window.[130] The event need not be seen or observed, but may still be explained by established knowledge, in this case, criminal behaviour. Abductive reasoning therefore offers a

[125] Huffington Post (12 June 2018) At the CIA, a fix to communications system that left trail of dead agents remains elusive. Available at: https://www.huffingtonpost.com/entry/at-the-cia-a-fix-to-communications-system-that-left-trail-of-dead-agents-remains-elusive_us_5c094117e4b069028dc7696a [accessed 15 March 2019]; Yahoo News (2 November 2018) The CIA's communications suffered a catastrophic compromise. It started in Iran. Available at: https://in.news.yahoo.com/cias-communications-suffered-catastrophic-compromise-started-iran-090018710.html?guccounter=1 [accessed 3 November 2018]; Dorfman, Z. (15 August 2018) Botched CIA communications system helped blow cover of Chinese agents, *Foreign Policy.* Available at: https://foreignpolicy.com/2018/08/15/botched-cia-communications-system-helped-blow-cover-chinese-agents-intelligence/ [accessed 1 November 2018].
[126] Wikileaks (7 March 2017) Vault 7: CIA Hacking Tools revealed. Available at: https://wikileaks.org/ciav7p1/ [accessed 23 December 2020].
[127] Gill, P. 'Theories of intelligence', in *The Oxford Handbook of National Security Intelligence, edited by Loch K. Johnson,* (Oxford, Oxford University Press, 2010), p. 44.
[128] Timmermans, S. & Tavory, I. 'Theory construction in qualitative research: from grounded theory to abductive analysis', *Sociological Theory,* 30:3, 2012, p. 171.
[129] Gill, P. 'Theories of intelligence', p. 44.
[130] Walton, D. *Abductive reasoning,* (Tuscaloosa, The University of Alabama Press, 2005), p. xiii.

middle road between deductive and inductive reasoning, formulising means of conjecture to make new discoveries.[131] Whereas deduction tests the validity of hypotheses by logically deducting premises, and induction draws general conclusions from specific premises, abduction, as characterized by Walton, is the process of academic guessing, or *finding the right guess*.[132] As Pierce explained, "Deduction proves that something must be; Induction shows that something actually is operative; Abduction merely suggests that something may be." [133] Put another way, deduction provides answers to "why" questions, induction offers answers to "what" questions, and abduction offers *plausible* answers to both, offering an invaluable source of discovery where no other methods of reasoning suffice.[134]

Abduction is often considered the weakest of the three forms of reasoning, limited only to plausible explanations.[135] Nonetheless, understanding what *may* be, rather than what *is,* can be a powerful form of discovery, opening doors to 'see things that we might miss by staying with tried-and-true explanation.'[136] This is particularly acute for international relations, which cannot be fully explained by deduction or induction alone.[137] By applying history to uncover 'new connections and relations that are not directly observable', scholars 'analyse already known occurrences in a novel way'.[138] Crucially, in intelligence studies history is regarded as a necessary pathway to making sense of the secret world.[139] As Gill explains:

---

[131] Ibid, p. 7.
[132] Ibid, p. 9-10.
[133] Ibid, p. 7.
[134] Blaikie, N. *Designing social research: the logic of anticipation* (Cambridge, Polity Press, 2010), p. 107.
[135] Shank, G. 'Abduction', in *The SAGE Encyclopedia of Qualitative Research Methods*, edited by Lisa M. Given (London, SAGE, 2008), p. 1.
[136] Ibid.
[137] Ben-Haim, Y. 'Positivism and its limitations for strategic intelligence: a non-constructivist info-gap critique', *Intelligence and National Security*, 33:6, 2018, p. 913.
[138] Gill, P. & Phythian, M. *Intelligence in an insecure world*, p. 26.
[139] Moran, C. 'The pursuit of intelligence history: methods, sources, and trajectories in the United Kingdom', *Studies in Intelligence, CIA*, 55:2, 2011, p. 45-56; Omand, D. 'Learning from the secret past',

> Historical accounts are the bedrock for our work but much of the intelligence process cannot be observed – especially not through the prism of official documents - and thus we must also develop speculative hypotheses that can be tested against the evidence rather as doctors do as they test out different diagnoses.
>
> In this process of "abduction," "by applying alternative theories and models in order to discern connections that were not evident, what intelligence scholars are doing is what good intelligence analysts do – but in doing so neither group is merely describing reality as if through clear glass. They are seeking to make sense of and thus actively 'create' the worlds of intelligence and government"[140]

Without these historical lessons, much in intelligence would remain opaque, to the detriment of scholars and practitioners alike. But while the past is a useful tool for interpreting the present, it does carry pitfalls, since '[one] can ransack history to prove damn near anything'.[141] History should be used as a 'starting point', providing guiding lessons rather than a 'list of prescriptions to be rote-learned or written down in training manuals.'[142] As Caddell and Caddell elaborate:

> An instructor also should avoid prescriptive interpretations that pin the blame (or award the credit) of a case on a single individual, organization, or action. Rarely (if ever) is it the case that 'fixing Problem X would change everything' or that 'everything would have been different if only decision-makers had listened to this single report' (which they may or may not have been shown) … Lessons, if there are any to be had, should be arrived at only as a byproduct of thoroughly interrogating the facts at hand … not force-fed and regurgitated in fill-in-the-blank fashion.[143]

Properly applied, history should be used to derive 'holistic' considerations of causation, honing on underlying causal mechanisms, their anticipated effects, and the conditions necessary for those causal mechanisms to come into effect.[144] In the social sciences, such historical analyses usually pertain to the influence of structures (causal

---

in *Learning from the Secret Past: Cases in British Intelligence History,* edited by Robert Dover and Michael S. Goodman (Washington, Georgetown University Press, 2011), p. 1-7.

[140] Gill, P. 'Theories of intelligence', p. 44.

[141] Caddell, J. Jr & Caddell, J. Sr. 'Historical case studies in intelligence education: best practices, avoidable pitfalls', *Intelligence and National Security,* 32:7, 2017, p. 892.

[142] Scott, L. & Hughes, G. 'Intelligence, crises and security: lessons from history?', *Intelligence and National Security,* 21:5, 2006, p. 660.

[143] Caddell, J. Jr & Caddell, J. Sr. 'Historical case studies', p. 898.

[144] Ibid, p. 892.

mechanisms) over human agency.[145] Structures, in this regard, may vary dependent upon the study in question, but can range from practices and institutions, to the social and political, all of which influence the decisions of individuals or collective actors.[146] By defining structures through abduction, analysts can reveal the 'conditions of existence or "rules of the game" of social action', looking beneath 'given appearances to the underlying social relationships that generate … phenomenal norms.'[147] Thus, by drawing causal mechanisms from history, analysts can better explain actors' decisions, while in turn, scholars of intelligence can apply similar logic to "create" the realities of the secret state, as Gill and Phythian illustrate:

> For example, in examining the actions of intelligence officers, one issue is how they view procedural rules and laws. Whether they view them as empowering or constraining will have some effect on their conduct – their original intention to act in a given situation may be reinforced, they may decide to act differently within the rules, act outside of the rules, or not act at all.
>
> In turn, these (in)actions may have short- or long-term implications for the rules – they may be seen as providing useful legal protection for officers, as unwieldly, or as so restrictive as to require amendment.[148]

This 'critical realist' approach acknowledges that underlying structures (or causal mechanisms) are influential, but not necessarily directly observable, and therefore require discovery.[149] Critical realists perceive a reality shaped by influential factors which cannot always be observed but, under contingent conditions, hold a tendency to produce certain outcomes.[150] Within this 'structured reality', knowledge cannot be produced by clinging to 'actors' accounts or record-keepers' notes', rather, scholars must engage their imaginations to determine causal mechanisms and their outcomes.[151]

---

[145] Gill, P. & Phythian, M. *Intelligence in an insecure world,* p. 27-28.
[146] Ibid.
[147] Wendt, A. E. 'The agent-structure problem in international relations theory', *International Organization,* 41:3, 1987, p. 363.
[148] Gill, P. & Phythian, M. *Intelligence in an insecure world,* p. 27-28.
[149] Ibid.
[150] Lawson, J. M. *Critical realism and housing research,* (London Routledge, 2006), p. 19.
[151] Ibid.

Moreover, while abduction is considered to be at its most effective when explaining known occurrences in a novel way, this critical realist perspective also implies predictive capacity. Abductive prediction has, however, invoked ample scepticism within critical realist camps, since, in contrast to the natural sciences, the social world consists of open systems that fluctuate over time.[152] Consequently, some critical realists outright reject predictive utility in the social sciences, as while the closed conditions of the natural sciences enable predictive accuracy, in open conditions 'generative mechanisms (that is, causal powers and the processes by which these powers work) operate in combination, making it difficult or impossible to predict the specific outcome in each case.'[153] One central issue is society's tendency to learn, adapt, and self-change, often as a consequence of knowledge generated through the social sciences.[154] Critical realists aim to generate new knowledge for 'savvy' actors to use in 'transformative ways', but by doing so they contribute to society's tendency for self-change, making accurate prediction a self-defeating pursuit.[155] By comparison, predictions within the sciences can be drawn from tightly controlled circumstances, offering greater levels of accuracy compared to chaotic open systems.[156]

Nevertheless, through the analysis of known events, it is considered possible to draw out 'hitherto unrealized potentials', creating plausible interpretations of the future.[157] According to Jackson, this form of reasoning is barely prediction in the classic sense of its meaning, '[saying] that something *could* happen is not the same as saying that it *will* happen, and critical realism … stands firmly on the side of the

[152] Næss, P. 'Prediction, regressions and critical realism', *Journal of Critical Realism,* 3:1, 2004, p. 133.
[153] Ibid, p. 157.
[154] Ibid.
[155] Jackson, P. T. *The conduct of inquiry in international relations: philosophy of science and its implications for the study of world politics,* (London, Routledge, 2011), p. 121-122
[156] Wynn, Jr. D. & Williams, C. K. 'Principles for conducting critical realist case study research in information systems', *MIS Quarterly,* 36:3, 2012, pp. 793-794
[157] Jackson, P. T. *The conduct of inquiry in international relations,* p. 121-122.

former.'[158] But some critical realists see merit in this limited form of prediction, believing it can, and should, be attempted within social science.[159] As Sayer's argues, "in so far as it stimulates action this may be better than having no prediction."[160] He reasons that while flawless predictions are unlikely in social science, they can still hold value if ascribed to conditionally dependent interpretations of the future.[161] In other words, abductive prediction works if the circumstances into which mechanisms are applied are clearly demarcated, and the operation of those mechanisms are presupposed. This offers the opportunity to weigh future outcomes if these conditions remain consistent, while providing a useful means to consider 'what we must make or prevent' if specific goals are to be achieved.[162]

Næss adds to this logic with two further arguments. First, critical realism is better suited for predicting the effects of causal mechanisms, more so than the situations that might arise as a result of those effects.[163] While 'effects' can be reduced to a number of possible consequences, 'situations' in an open system are affected by a far greater number of social and political variables. Consequently, predictions must focus on a direction of influence (whether a certain effect is more or less likely), through 'crude qualitative assessments', which minimise the potential number of uncertainties.[164] In contrast, attempts to accurately predict events that might manifest as a consequence of those effects, would involve too many uncertainties.[165] As Ben-Haim illustrates, analysts, to a degree of accuracy, could doubtlessly envision the immediate effects of global sea level rising (e.g. crop devastation or mass migration).[166] However,

[158] Ibid
[159] Næss, P. 'Prediction, regressions', p. 157
[160] Ibid.
[161] Sayer, A. *Method in social science: a realist approach* (New York, Routledge, 1992), p. 137.
[162] Ibid.
[163] Næss, P. 'Prediction, regressions and critical realism', p. 157-161.
[164] Ibid.
[165] Ibid.
[166] Ben-Haim, Y. 'Positivism and its limitations for strategic intelligence, p. 913.

to predict precisely what policies nation states will enact as a consequence of those effects, or what conflicts would arise, requires an incalculable number of variables. This leads into Næss's second argument, that certain social systems are quasi-open, meaning the conditions necessary for particular effects are likely recurrent in the foreseeable future.[167] The fact remains that analysts cannot foresee every variable (for instance, a sudden asteroid strike), but critical realism's crude conditional predictions hold greater value if key conditions are likely to remain consistent over time. To illustrate, it could be assumed that a strong, stable, liberal democracy would be unlikely to change political models in the foreseeable future, but that doesn't rule out the possibility that such an outcome might eventuate.

If necessary assumptions are made, it is possible to assess the value of technology to espionage in the present and foreseeable future. The limitations of this critical realist approach, however, infer that such reasoning can only dictate the direction of effect, not the exact scenarios that will emerge as a result of those effects. Specifically, by focusing on the effects of causal mechanisms, it is, on the one hand, possible to make assessments as to whether technology is likely to prove advantageous for espionage. Yet it is not possible to determine its specific implications, such as the exact political or operational consequences that will arise as a result of cyberspace's advantage (or disadvantage). In other words, abduction can estimate the odds of failure, but it cannot determine the precise fate of Agent X under circumstance Y, nor can it accurately predict the next Cuban Missile Crisis. Simply put, abduction can offer probabilistic outcomes as to what cyber-enabled tradecraft might mean for the espionage world, but that is as far as its predictions can be pushed. That being said, in keeping with critical realism's limited predictive capacity, several critical conditions

[167] Næss, P. 'Prediction, regressions and critical realism', p. 148 & 157-158.

must be assumed in order to ascertain any final conclusions. First, is the assumption that intelligence officers will recognise technology's opportunities and limitations. Second, is the assumption that opponents will seek to protect their secrets in accordance with the behaviour of a hard target state. Since either side has a vested interest in gaining an advantage over the other, it seems logical for both of these assumptions to remain true; nonetheless, conditions can change over time, meaning we must presume that the status quo is maintained for outcomes to remain true.

To draw these abductive lessons, a suitable case study must first be selected, yet from the very outset it is clear that such a case must carry relevance to the problem at hand. As a consequence, any suitable case must exhibit a varied range of tradecraft in application, while offering clear insights into why they failed or succeeded. Moreover, it is also necessary that street surveillance (in this sense pertaining to the identification and tailing of intelligence officers) be a core driver for the very application of said tradecraft, since its capacity to compensate for an inability to meet interpersonally is the central issue of this study. Moreover, even if relevance is clear, such a case must also account for issues in historical sources, which are often muddied by official secrecy.[168] For example, if a window into events is only offered through official disclosures, then historians risk being fed a misleading or outright fabricated narrative that cannot be cross-examined, as Scott and Jackson argue:

> Richard Aldrich has cautioned against interpreting the official records of the Public Record Office 'as an analogue of reality'. He has argued persuasively that British archives are a highly manipulated source of evidence for historians. The British government's success in controlling knowledge of its wartime achievements in signals intelligence and strategic deception is a good example of official policy shaping the parameters of historical enquiry. There are almost certainly other such cases that have yet to come to light.[169]

[168] Caddell, J. Jr & Caddell, J. Sr. 'Historical case studies', p. 893
[169] Scott, L. & Jackson, P. 'The study of intelligence in theory and practice', *Intelligence and National Security,* 19:2, 2004, p. 145.

While this risk is more pertinent to states who manipulate the public narrative, e.g. 'Soviet security and intelligence services', it nevertheless should not be discounted when dealing with US and British records.[170] Even if such documents are not doctored, there are risks that the 'full' picture, including in documents potentially sensitive or damning, especially in the context of sources and methods, might be excluded from the reader's purview.[171] For example, MI5's official historian, Christopher Andrew, was met with some criticism for his unparalleled 'Ivory Tower' access to MI5's secret records, which cannot be contested or cross-examined if restricted to the bulk of historians.[172] Scepticisms of this fashion are particularly acute for those accounts by former practitioners, which can be muddied by intelligence bodies or skewed to meet personal or political agendas. Kim Philby's *My Silent War* or Peter Wright's *Spycatcher* underscore the risks of unverifiable accounts, hence why Scott and Jackson regard the value of memoirs as 'an open question'[173]

Therefore, in addition to relevance to the phenomena under investigation, a suitable case requires satisfactory primary and secondary data.[174] To that effect, it is paramount to avoid 'instant histories', 'oversimplified narratives', or ''pop up' cases', cases, that are either too recent, brief, or anecdotal to have garnered sufficient research or offer nuanced findings.[175] As Caddell and Caddell illustrate, a study of the Cuban Missile Crisis would have been impossible during the mid-1960s, since capabilities that played a significant role in the event were classified at the time. A fitting case must offer multiple perspectives, supported by extensive disclosures, over a period of time

[170] Ibid.
[171] Ibid.
[172] Moran, C. 'The pursuit of intelligence history', p. 46.
[173] Ibid, p. 35-36; Scott, L. & Jackson, P. 'The study of intelligence', p. 145.
[174] Caddell, J. Jr & Caddell, J. Sr. 'Historical case studies', p. 893.
[175] Ibid, p. 898-901.

long enough to have produced sufficient evidence of causal mechanisms in play.[176] But such demands can skew case selection towards 'more salacious events', since instances of outright failure, incompetence, or abuse 'are more likely to have drawn scrutiny and research.'[177] However, while it is considered common wisdom that we learn more from failures than successes, it bears note that overreliance on either failure or success carries risk, by overstating or understating the significance of variables and conditions beyond that particular case. There is no single recipe to find balance here, with cases of equal failure and success unlikely, but it is nonetheless important to include perspectives from either angle where possible.[178]

In this regard, the case of espionage against the Soviet Union throughout the mid-late years of the Cold War (post-1960) will be selected. As will be unpacked in chapter 4, this decision rests on three factors. First, in terms of relevance, throughout this era technology began to play a critical role in HUMINT affairs, driven by the need for solutions to the KGB's street surveillance panopticon.[179] Second, due to the length of the period and the time since its passage, the Cold War meets Caddell and Caddell's criteria for enough 'historical time', increasing the likelihood of useful primary and secondary data.[180] Simply put, the events of this era were sensational enough to draw considerable inquiry by historians and practitioners alike, and are old enough to have experienced substantial declassifications, offering a more complete picture in comparison to more contemporary events. Consequently, this period avoids the pitfall of 'instant histories', by offering a girth of perspectives, claims, and experiences.[181] And third, while intelligence agencies failed in this period to recruit a sufficient number

[176] Ibid.
[177] Ibid, p. 894
[178] Ibid, p. 898.
[179] Wallace, R. et al. *Spycraft*, p. 51-54; Macrakis, K. 'Technophilic hubris', p. 147.
[180] Caddell, J. Jr & Caddell, J. Sr. 'Historical case studies', p. 891.
[181] Ibid, p. 897-898.

of sources, they did succeed in recruiting at least a handful of valuable agents, many of whom continued their espionage for several years until their eventual betrayal, thereby offering perspectives of both failure and success.[182] Through examining this case, this study will show that human behaviour is the defining factor of tradecraft's success or failure, leading to the following hypothesis:

- Justifying and mitigating the risks of tradecraft (and technology) in hard target conditions requires greater trust in the behaviour of the prospective or serving spy. Yet, in such conditions the odds of failure are vastly increased since intelligence officers are less able to meet their sources and agents and have less influence over, and insight into, their behaviour.

Evaluation

This chapter has presented the conceptual, literary, and methodological foundations of this project. It proposes that espionage is distinguished from intelligence collection more broadly by its human emphasis, but it is concurrently distinct from human intelligence by its narrowed focus. Unlike imagery satellites or diplomatic gossip, espionage pertains to clandestinely acquired sources who maintain authorised access to secret information. Those 'agents' are enabled by foreign intelligence officers, who recruit and handle spies through a series of methods known as tradecraft. But since intelligence is a competitive world, all espionage competes with counterintelligence, which encompasses a cocktail of offensive and defensive activities designed to detect and neutralise foreign intelligence operations.

It further argued that cyberspace is a convergence of interconnected technologies and their subsequent human interactivity. While often confused with the Internet, its scope is far wider, carrying providing revisions through state, military, and

[182] Russel, R. L. *Sharpening strategic intelligence: why the CIA gets it wrong and what needs to be done to get it right*, [Kindle version] (New York, Cambridge University Press, 2007), p. 51-52; Mendez, A. et al. *The Moscow rules,* p. 174.

intelligence affairs, a point underscored by its incorporation into military doctrine as a new domain for warfare alongside land, air and sea. Its impact on intelligence too has been profound, leading to the emergence of an entirely new form of collection derivatively known as cyber espionage. But while cyberspace has changed the intelligence world indelibly, cyber espionage is not classic espionage; one pertains to hacking, the other pertains to human sources. And it is the latter's evolution in the cyber era that constitutes the focus of this study.

It also showed that while much has been written about technology's effects on intelligence, its specific role in espionage remains a somewhat niche area of scholarship, continuing a trend of tradecraft's academic neglect. But while the impact of cyberspace on espionage remains an underdeveloped line of inquiry, there is no shortage of profound assumptions. Although there is strong evidence to show that personal meetings will remain an important aspect of espionage, cyberspace is seen to carry a vast and potentially game-changing array of affects. These perceived advantages, as categorised under the four key functions of tradecraft (recruitment, surveillance, handling, and collection) are seen to make espionage faster, more secure, and more wide-reaching than ever before. The assumptions made in this literature are, however, notably uncritical, focused largely on its *positive* elements without sufficient consideration for its limitations. Only a handful of scholars, Althoff, Sano and Tucker, remain sceptical, but in their view technology is just another variable to be targeted by counterintelligence, and is fundamentally vulnerable to the influence of human behaviour. Thus, this polarity between what this thesis labels the *optimists* and *pessimists* must be resolved if cyberspace's impact is to be understood.

To address this gap while overcoming the official secrecy problem, this chapter proposed an abductive approach. There is ample data pursuant to cyberspace itself, but

no pre-existing framework to interpret or navigate this information. As such, guiding lessons drawn from history offer a conceptual basis through which to understand the unobservable. While abduction, as an academic form of speculation, is considered to be the weakest form of reasoning, it is nevertheless an established means of determining *probabilities*, and a vital tool for intelligence scholars and analysts alike. Abductive reasoning essentially constructs reality through a critical realist perspective, by understanding causal mechanisms and their anticipated effects. Just as intelligence analysts use abduction to understand the behaviour of foreign actors and anticipate their decisions, so too do intelligence scholars use abduction to understand its processes, by imagining what will *likely be* rather than *what is*. These holistic considerations of causation, or lessons, must guide rather than prescribe any construction of reality, and in turn, they offer predictive utility. While it is impossible to accurately determine future events within chaotic open systems, it is possible to draw crude qualitive assessments of the future. These, built on the basis of vital assumptions, allow technology's impact to be considered far beyond its current effects, opening a window into the short and long-term future of espionage.

It further showed that in deriving these lessons, a case must first offer suitable relevance the problem at hand, meaning it must clearly exhibit the applied successes and failures of tradecraft for the purpose of resolving a surveillance problem. The selection of such a case must give weight to several problems of research, not least the same barrier of official secrecy that placates contemporary scholarship. Cases that are focused on events that are too narrow, too recent, or too anecdotal, cannot provide the necessary detail for a sufficient causal analysis. What is required is a broad, detailed case study supported by a girth of primary and secondary data, allowing for multiple

perspectives to be scrutinised and compared. Consequently, as will be explored further ahead, the Cold War offers an ideal case study.

Chapter 2
Espionage and the 'resurgence of state based threats'

Introduction

Since the purpose of this thesis is to assess espionage's ability to 'pierce these hard target states', it is necessary to establish why this matters. This chapter thus seeks to understand the current state of security affairs, and the changing, or evolving, role of espionage. There are two important factors to consider, first is the re-emergence of Cold War rivalries between nuclear powers, and second is the intelligence community's response. It will argue that parallel to shifting strategic policy, the intelligence community will need to refocus more of its resources from counterterrorism, which has dominated security agendas for three decades, back towards nation state targets. As Western relations with Russia and China continue to decline, this chapter will show that the importance of espionage is concurrently rising.

The chapter begins by examining the key issues that have elevated Russia and China to the top of strategic agendas. It examines both conventional geopolitical rivalries and areas of potential conflict, and the more insidious challenges posed by their aggressive and increasingly ambitious covert operations. Particular emphasis is placed on the circular nature of declining relations, by underscoring how Moscow and Beijing's perceptions of Western containment, which is in response to their own aggression, has encouraged hostile and expansionist behaviour. In addition, it will explore how the perils of such confrontation are being worsened by systemic attempts to plunder economic secrets, penetrate classified networks, and subvert the foundations of Western democracy. It thus establishes the new security landscape, putting Russia and China at the very top of the political agenda.

In turn, the role of espionage in addressing these challenges will be closely examined, by providing a conceptual assessment of the strengths and weaknesses of alternative collection methods in the context of these hard targets. Specifically, the limitations of open sources and technical intelligence will be closely scrutinised, taking into accounts the resources and skillset of Russia and China's vast counterintelligence apparatus. It will argue that where high valued information is concerned, such as the internal workings of the Kremlin, or the intentions behind a sophisticated Chinese hack, there is no substitute for the spy, thus proving the case for espionage as an increasingly necessary line of defence. It will conclude by examining the intelligence community's response, as they shift towards this new reality.

The military threat from Russia and China

With the dissolution of the Soviet Union, early expectations for a more cooperative, US-dominated international order were largely optimistic, 'Russia appeared to have been so weakened by political, economic, and military collapse as to be finished as a shaper of world affairs.' [1] The decline of Soviet communism, and the end of ideological polarities that defined the Cold War, opened the possibility for renewed cooperation between former rivals.[2] This optimism soon proved misjudged, as reality began to echo the more sceptical view that relations with post-Soviet Russia would be distinctly competitive.[3] Under the leadership of President Vladimir Putin, Russian foreign policy is increasingly perceived as 'aggressive, nationalistic and threatening', as the Kremlin strives 'to challenge the post-Cold War order'.[4]

[1] Mankoff, J. *Russian foreign policy: the return of great power politics*, (Lanham, MD, Rowman & Littlefield Publishers, 2012), p.7.
[2] Cross, S. 'NATO-Russia security challenges in the aftermath of Ukraine conflict: managing Black Sea security and beyond', *Southeast European and Black Sea Studies*, *15:2, 2015,* p. 152.
[3] Ibid.
[4] Mankoff, J. *Russian foreign policy,* p. 6.

Much friction has been attributed to NATO expansionism, which Russia perceives as a direct threat to its own hegemony.[5] Early signs of trouble emerged in the 2008 Georgian war, which was 'interpreted in the West as Russia's way of stopping the spread of NATO'.[6] The serving Russian president at the time, Dmitri Medvedev, proclaimed that the war had successfully curbed NATO's efforts to absorb Russia's neighbours into its alliance, telling soldiers "a number of countries which (NATO) tried to deliberately drag into the alliance, would have most likely already been part of it now."[7] Yet, Russia's entrenched concerns of NATO enlargement are only a subset of a broader polarity in regional strategic perceptions.[8] There are firm beliefs among Russia's 'security and foreign policy elite that in a highly competitive and increasingly conflictual world, western political ideals and regional structures mask strategic goals.'[9] As a consequence, the Kremlin views itself in competition with an increasingly consolidated, US-dominated Western opposition, which does not share Russia's strategic ambitions or security concerns.[10]

As relations with the West decline, the Kremlin has grown more emboldened on the world stage, with its incursions into Syria interpreted as an attempt to cement Russia's strategic position in the Middle East.[11] Allison contends that Russia's intervention was derived from its close relationship with Iran, rather than Syria, as the Kremlin perceived the Syrian civil war as masking Western strategic ambitions against its Iranian partners.[12] In the view of the Russian foreign minister, Sergey Lavrov, the

[5] Cross, S. 'NATO-Russia security challenges', p. 152.
[6] Nodia, G. 'The revenge of geopolitics', *Journal of Democracy*, 25:4, 2014, p. 146.
[7] Reuters (21 November 2011) Russia says Georgia war stopped NATO expansion. Available at: http://in.reuters.com/article/idINIndia-60645720111121 [accessed 30 October 2017].
[8] Allison, R. 'Russian 'deniable' intervention in Ukraine: how and why Russia broke the rules', *International Affairs,* 90:6, 2014, p. 1256.
[9] Ibid.
[10] Ibid.
[11] Allison, R. 'Russia and Syria: explaining alignment with a regime in crisis', *International Affairs,* 89:4, 2013, p. 795.
[12] Ibid, p, 808.

West's oppositions to Assad was "a cover for a grand geopolitical game … Many have in mind not so much Syria as Iran. They openly say that it is necessary to deprive Iran of a very close ally."[13] Russia's ties with Iran are historically close, as the two share common ground over issues ranging from trade to regional security, opposition to regional Western / NATO expansion, oil and gas extraction in the Caspian Sea, Iran's nuclear programme, Middle Eastern influence, counterterrorism, and relations with Turkey, all of which helped an increasingly isolated Russia to justify military involvement in Syria's complex civil war.[14]

However, Russia's willingness to challenge the West's strategic objectives via military action was further displayed by its 2014 incursions in Ukraine and the annexation of Crimea. Although concerns about Ukraine's prospective NATO membership raised obvious alarms in the Kremlin, the conflict also reflected Russia's declining relations with the European Union.[15] While modern Russia's relationship with the EU began on strong footing, their ideological differences soon began to fracture relations, 'as Europe and Russia drew closer they realised just how different they were.'[16] Prior to 2014, Ukraine had been closer to Russia than Europe, and even rejected NATO membership, but the 2014 overthrow of President Yanukovych led to a sudden shift in course.[17] Consequently, Russia's elite interpreted the revolution as a Western coup, as underscored by Putin himself:

> Moreover, in the framework of the EU Eastern Partnership Program there have been attempts to tear states which had been parts of the former USSR off Russia and to prompt them to make an artificial choice "between Russia and Europe." The Ukrainian crisis has become a high point of these negative trends. We repeatedly warned the USA and its western allies about harmful consequences of their interference in Ukrainian domestic affairs but they did not listen to our

[13] Ibid.
[14] Nalbandov, R. *Not by bread alone: Russian foreign policy under Putin*, (Lincoln, Nebraska, Potomac Books, 2015), p. 431-432.
[15] Allison, R. 'Russian 'deniable', p. 1256
[16] Sakwa, R. *Frontline Ukraine: crisis in the borderlands,* (London, I.B. Tauris, 2014), p. 55.
[17] Ibid; Allison, R. 'Russian 'deniable', p. 1256-1257.

opinion.[18]

This may help explain why Russia seized the initiative through a war of deniability, absorbing Crimea and strengthening its regional power.[19] Taking Crimea under its sovereignty also carried significant military benefits, giving Russia full control of a number of highly defensible sea ports, including Sevastopol.[20] Reclaiming Sevastopol constituted a considerable victory for Putin, as even if the regional security benefits of the Crimea were put aside, its deep entrenchment in Russian history make it unlikely to be conceded.[21] But in terms of a wider strategic picture, the ongoing low-intensity conflict in Ukraine, and the latter's determination to reclaim Crimea, means the threat of Ukrainian membership in NATO is essentially over.[22]

Russia's actions in Ukraine caused substantial damage to West / Russia relations.[23] As asserted by MacFarlane and Menon, it reflected 'the most significant security crisis in Europe since the collapse of the Soviet Union'.[24] It occurred at a point

[18] President of Russia (9 February 2015) Interview to Al-Ahram daily. Available at: http://en.kremlin.ru/events/president/news/47643 [accessed 30 October 2017].
[19] Freedman, L. 'Ukraine and the art of limited war', *Global Politics and Strategy*, 56:6, 2014, p. 12-17.
[20] Before 2014, the Black Sea Fleet had leased Sevastopol basing rights from the Ukraine administration, yet this third-party reliance impeded Russia's plans to modernize its regional military and naval forces. As Delanoe argues, 'Moscow is now fully able to commission new vessels and dispatch new military hardware, including coastal artillery and land-based forces and aircraft'. For more details, see Delanoe, I., 'After the Crimean crisis: towards a greater Russian maritime power in the Black Sea', *Southeast European and Black Sea Studies*, 2014, p. 375.
[21] Len Scott has argued that Sevastopol's history must be factored in when calculating Putin's rationale. He told press "Crimea, it should not be forgotten was never part of the Ukraine until 1954, when Nikita Khrushchev handed it over as a gesture to commemorate 300 years of Russian-Ukrainian relations. The people of the Crimea had no say in Khrushchev's decision", adding "[many] Russians see the siege and battle of Sevastopol almost in the same way as they see the siege of Leningrad and the battle for Stalingrad. Sevastopol was an enormous and ferocious battle, about which we know very little in the West." For more details, see WalesOnline (20 March 2014) The carnage in Crimea during World War II has shaped Putin's response to Ukraine crisis, argues Welsh historian. Available at: http://www.walesonline.co.uk/news/wales-news/memories-carnage-crimea-during-world-6851251 [accessed 31 October 2017].
[22] Pifer, S. 'Will Ukraine join NATO? A course for disappointment', *Brookings* 25 July 2017. Available at https://www.brookings.edu/blog/order-from-chaos/2017/07/25/will-ukraine-join-nato-a-course-for-disappointment/ [accessed 30 October 2017].
[23] Monaghan, A. *The new politics of Russia: interpreting change,* [Open Access e-book] (Manchester, Manchester University Press, 2016), chapter 2.
[24] MacFarlane, N. & Menon, A. 'The EU and Ukraine', *Survival: Global Politics and Strategy,* 56:3, 2014, p. 95; Allison, R. 'Russian 'deniable', p. 1255.

when Western / Russian relations had already reached the proverbial cliff edge, thereby reducing opportunities for a diplomatic solution.[25] In response, the US and EU implemented stringent economic sanctions, which occurred during a period of falling oil prices, and further fuelled downward pressure on the struggling rouble.[26] However, the prospect of an interventionist military response by NATO has been compounded by Russia's projection of power, which relies on low-level, deniable conflict backed by the threat of nuclear escalation.[27] This latter point is critical, as while other nations sought to reduce their highly expensive and politically tumultuous nuclear arsenals, Russia has recently expanded its post-Cold War nuclear prowess, with at least 2,000 tactical nuclear weapons allegedly ready for delivery.[28]

This nuclear dimension makes forceful response increasingly dangerous, particularly to aggression against a NATO member state.[29] Russia, in turn, has sought to monopolize on these concerns, sending nuclear bombers close to, or into, NATO airspace, brazenly signalling its defensive readiness.[30] But this nuclear grandstanding is only worsened by a lack of clarity regarding Russia's strategic objectives.[31] Although 'there is no indication that Putin has immediate design on outright control of NATO member states', it would also be 'imprudent … for NATO to rule out such a contingency as beyond the realm of possibility.'[32] These points have been increasingly echoed in Western strategic documents, with the UK's 2015 *National Security Strategy*

[25] Monaghan, *The new politics of Russia*, chapter 2.
[26] Rutland & Middletown note that Russia's government expected - in late 2014 - that the sanctions would cost $40 million over the course of the year, followed by another $100 billion in falling oil prices. For more details, see Rutland, P. & Middletown, CT. 'The impact of sanctions on Russia, *Russian Analytical Digest,* 157, 2014, p. 4.
[27] Kroenig, M. 'Facing reality: getting NATO read for a new Cold War', *Survival; Global Politics and Strategy,* 57:1, 2015, p. 53-54.
[28] Ibid.
[29] Kroenig, M. 'Facing reality', p. 56-57; Cross, S. 'NATO-Russia security challenges', p. 153.
[30] BBC News (5 October 2016) NATO jets scrambled as Russian bombers fly south. Available at: http://www.bbc.co.uk/news/world-europe-37562499 [accessed 31 October 2017].
[31] Kroenig, M. 'Facing reality', p. 53.
[32] Ibid.

stating that 'we cannot rule out the possibility that [Russia] may feel tempted to act aggressively against NATO Allies.'[33] Similarly, according to the White House, Russia is seen to be endangering 'international norms that have largely been taken for granted since the end of the Cold War'.[34] At a time of such hostility, the odds of conflict erupting or crises escalating are multiplied, meaning all sides must exercise caution and restraint.[35] But cooperation, as the EU has experienced, is proving increasingly difficult between two sides marred by a widening 'values gap', as the Kremlin's approach to democracy, human rights, and 'the role of state in society', further sours opportunities to resolve wider strategic issues diplomatically.[36]

While Russia's geopolitical proximity to Europe and its incursions in Syria and Ukraine have clearly increased the likelihood of conflict, the threat posed from China continues to incite fears of an inevitable superpower clash.[37] Cemented by what Beeson and Li describe as the 'liberalization of the domestic economy' and the 'reintegration into the global economy', China has emerged as the world's second largest economic power.[38] To a degree, China's rise has been notably peaceful, marked by Beijing's efforts to seek 'positive affirmation from the international society.'[39] With the collapse of the Soviet Union, US policymakers hoped for a new era of cooperation, viewing Beijing as a possible ally against the rising dangers of terrorism and WMD

[33] HM Government (November 2015) National security strategy and strategic defence and security review 2015, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf [accessed 31 October 2017], p. 18.
[34] The White House (1 February 2015) National security strategy. Available at: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf [accessed 31 October 2017], p. 10.
[35] Cross, S. 'NATO-Russia security challenges', p. 173.
[36] Monaghan, *The new politics of Russia,* chapter 2.
[37] Kissinger, H. 'The future of U.S.-Chinese relations', *Foreign affairs,* 91:2, 2012, p. 44-45.
[38] Although China's economic reforms began in the 1970s, they only gained 'momentum' in the 1990s, coalescing with the Cold War's ending. Beeson, M. & Li, F. 'What consensus? Geopolitics and policy paradigms in China and the United States', *International Affairs,* 91:1, 2015, p. 95.
[39] Yong, D. *China's struggle for status: the realignment*, (Cambridge, Cambridge University Press, 2009), p. 288

proliferation.[40] But as with Russia, this optimism proved misjudged, as China's economic and military power grew parallel to its alarming political ambitions.[41] While the turbulent relationship between the US and China today does not currently reflect the nature of confrontation with the Soviet Union during the Cold War, the 'parallels', as White contends, 'are clear and becoming clearer.'[42]

Steadily, relations between Washington and Beijing have devolved into zero-sum politics, with little trust between either party.[43] Chinese leaders, 'recalling the traumas of the collapse of the former Soviet Union', have 'become suspicious of US intentions to prevent China from rising to its rightful place' and are 'convinced that the US and the other Western countries have come together to encircle and undermine the Chinese regime.'[44] Early post-Cold War frictions soon arose due to China's asserted claim over Taiwan, '[for] decades, the issue of Chinese sovereignty over Taiwan has been considered to be the most plausible reason why the United States and China could come to blows.'[45] While China / Taiwan relations have somewhat improved (although they are far from resolved), Beijing's concerns over US military support for Taiwan are seen as direct drivers for its subsequent strategic initiatives.[46] In turn, China's efforts to strengthen its regional primacy against US hegemony have only provoked further escalation between both parties.[47] China has adopted an "anti-access=area-denial strategy", which entails modernising its military with a focus on denying opposing

[40] Friedberg, A. 'The future of US-China relations: Is conflict inevitable?' *International Security*, 30:2, 2005, p. 7.
[41] Yahuda, M. *The international politics of the Asia-Pacific,* (Abingdon, Routledge, 2006), p. 281.
[42] White, H. *The China choice: why we should share power,* (Oxford, Oxford University Press 2013), p. 115.
[43] Zhao, S. 'A new model of big power relations? China-US strategic rivalry and balance of power in the Asia-Pacific', *Journal of Contemporary China*, 24:93, p. 382.
[44] Ibid.
[45] McDevitt, M. 'The East China Sea: the place where Sino-U.S. conflict could occur', *American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy,* 36:2, 2014, p. 100.
[46] Ibid.
[47] Ibid, p. 100-101.

forces access to regional seas and airspace.[48] To support this strategy, Beijing is expanding its aircraft carrier programme and traditional naval forces, cyber capabilities, and anti-ship ballistic / cruise missiles, all designed to check regional US power.[49] In addition, China has upgraded its second strike nuclear capability which its leadership sees as 'an ultimate deterrent against the United States.'[50] Ergo, China may not have the 'absolute military capacities … formally equal to those of the United States', but it can pose 'unacceptable risks' should conflict erupt.[51]

Efforts to avoid escalation have only been worsened by the emergence of various sovereignty disputes over regional islands that are claimed by both Beijing and Washington's Pacific allies. [52] One dispute between China and Japan over sovereignty of the Senkaku / Diaoyu islands has become a potential 'new East China Sea Sino-U.S. flashpoint because of the U.S. security alliance with Japan.'[53] The islands, which are known to contain rich fishing grounds alongside oil and gas reserves, were historically owned by Japan, a claim that Chinese policymakers reject.[54] Beijing has also exacerbated tensions through its 'East China Air Defense Identification Zone', a parameter of air restriction that extends well into the disputed islands borders, which has been flatly rejected by the United States and Japan.[55] In response, Washington has criticized Beijing's "unilateral', 'provocative', 'coercive' and 'escalatory' action as attempts' to 'change the regional status quo', and 'has taken measured counter-actions

[48] Ibid; Dian, M. 'The pivot to Asia, Air-Sea Battle and contested commons in the Asia region', *The Pacific Review,* 28:2, 2015, p.243.
[49] O'Rourke, R. 'China naval modernization: Implications for U.S. Navy capabilities – backing and issues for Congress', *Congressional Research Service,* 2017, p. 2-3 & 50.
[50] Busynski, L. 'The South China Sea: oil, maritime claims, and U.S. – China strategic rivalry', *The Washington Quarterly,* 35:2, 2012, p. 145.
[51] Kissinger, 'The future of U.S.-Chinese relations', p. 45.
[52] Ibid, p. 48; Steinberg, J. & O'Hanlon, M. 'Keep hope alive: how to prevent U.S. – Chinese relations from blowing up', *Foreign Affairs,* 93:4, 2014, p. 108.
[53] McDevitt, 'The East China Sea', p. 101.
[54] BBC News (10 November 2014) How uninhabited islands soured China-Japan ties. Available at: http://www.bbc.co.uk/news/world-asia-pacific-11341139 [accessed 31 October 2017].
[55] Zhao, 'A new model of big power relations?', p. 377.

to check China's territorial advances', including sending 'a pair of American B52 bombers flying across China's newly declared Air Defense Identification Zone'.[56] Naval forces, ever present on the periphery, also serve as a reminder of the escalatory risks as Chinese fishing vessels continue to clash with Japan's coastguard.[57] Additional island sovereignty disputes have emerged in the South China Sea, between China and four Association of Southeast Asian Nations (ASEAN) - Indonesia, Malaysia, the Philippines, and Vietnam - all of whom hold regional defensive alliances with the US.[58] With, again, desire for the islands' oil, gas, and fishing reserves fuelling sovereignty claims, the problem has escalated, 'the issue has gone beyond territorial claims … the sea has started to become linked with wider strategic issues', pitting Chinese expansion and American regional power increasingly at odds.[59]

Although these East and South China Sea disputes may be manageable through diplomacy, 'all involved seem to fear that any show of restraint or accommodation will be taken as a sign of weakness, leading to even more assertive behaviour in the future.'[60] As such, the possibility that the US military may be drawn into a destructive conflict over far-away island disputes, has significantly increased.[61] This issue serves as a microcosm of a wider reality, that optimism for cooperation with Beijing has all but diminished.[62] According to China specialist, David Shambaugh, the "administration came in with one dominant idea: make China a global partner in facing global challenge", but now US policy makers "realize they're dealing with an increasingly

[56] Ibid.
[57] McDevitt, 'The East China Sea', p. 103.
[58] Buzynski, 'The South China Sea, p. 139.
[59] Ibid.
[60] Steinberg & O'Hanlon, 'Keep hope alive', p. 114.
[61] Goldstein, A. 'First things first: the pressing danger of crisis instability in U.S. – China relations', *International Security*, 37:4, 2013, p. 54-55.
[62] Landler, M. & Chan, S. (25 October 2010) Taking harder stance toward China, Obama lines up allies, *The New York Times.* Available at: http://www.nytimes.com/2010/10/26/world/asia/26china.html [accessed 31 October 2017].

narrow-minded, self-interested, truculent, hyper-nationalist and powerful country."[63] Currently, China's rising power carries enough weight to pose 'a direct challenge to America's strategic primacy', and posits a 'major structural transformation of the international system and the material distribution of power within it.'[64] These risks, combined with shrinking opportunities for de-escalation, have driven China to the very centre of Washington's agenda.[65]

Obama's 2012 Pivot Towards Asia underscored this emerging reality, which placed the Pacific at the forefront of US strategic policy.[66] The strategy aimed to send a clear message to Chinese policymakers that their aggressive regional expansion would be matched by a 'unified front'.[67] One dimension of this strategic rebalance has relied upon renewing regional coalitions and economic ties, , as Shambaugh adds, "[the] signal to Beijing ought to be clear … the U.S. has other closer, deeper friends in the region."[68] Similarly, the Pivot includes a major military reorientation, with the US shaping its regional power to directly countenance Beijing's strategic initiatives.[69] US military presence now rests on an 'operational concept defined Air-Sea Battle (ASB), aimed at rebalancing the Chinese military ascendency and to reaffirm the US primacy in the region'.[70] The strategy, which is clearly designed to check Beijing's aggression and surround China with US allies, has been widely interpreted as a policy of containment.[71] However, in circular fashion, the move is likely to 'worsen Beijing's

[63] Ibid.
[64] Beeson, M. & Li, F. 'What consensus?', p. 93.
[65] White, *The China choice'*, p. 114.
[66] Chen, R. 'A critical analysis of the U.S. "pivot" towards the Asia-Pacific: how realistic is neo-liberalism? *Connections,* 12:3, 2013, p. 39.
[67] White, *The China choice'*, p. 115.
[68] Landler, M. & Chan, S. (25 October 2010) Taking harder stance toward China, Obama lines up allies, *The New York Times.* Available at: http://www.nytimes.com/2010/10/26/world/asia/26china.html [accessed 31 October 2017].
[69] White, *The China choice'*, p. 114-115.
[70] Dian, M. 'The pivot to Asia', p. 237-238.
[71] Zhao, 'A new model of big power relations?', p. 383.

insecurity and fear of encirclement, accelerating the present security dilemma between China and the United States.'[72] The wider implications are far from optimistic, as argued by the head of the Joint Chiefs of Staff, China is likely to be America's "greatest threat" by 2025.[73] Similar sentiments have been echoed by General Michael Hayden, who claimed that China is well on the way to becoming the United States most significant existential threat, "if we do not handle the emergence of the People's Republic well, it will be catastrophic for the world."[74] The two sides appear to be locked in a ladder of escalation, and neither party is prepared to concede ground, thus for the foreseeable future the prospects of peace remain tentative at best.

The intelligence threat from Russia and China

Peaceful resolutions to what the US government describes as 'China's rise and Russian aggression', have been shortcoming.[75] Since diplomacy has proved unfruitful, and military action is unlikely to bode well for any party, it is perhaps unsurprising that Russia and China have sought to advance their foreign policy interests through their considerable intelligence resources.[76] Amongst the wide ranging issues posed by Russian and Chinese intelligence, cyber threats, particularly cyber espionage, which allows nation states to pilfer foreign secrets with profound outreach and relatively low

[72] Dian, M. 'The pivot to Asia', p. 238.
[73] CNN (27 September 2017) Top US general: China will be 'greatest threat' to US by 2025. Available at: http://edition.cnn.com/2017/09/26/politics/dunford-us-china-greatest-threat/index.html [October 31 2017]
[74] McGreal, C. (9 March 2016) America's former CIA chief: 'If we don't handle China well, it will be catastrophic', *The Guardian.* Available from https://www.theguardian.com/us-news/2016/mar/09/america-cia-nsa-chief-general-michael-hayden-china-catastrophic-for-world [accessed 12 October 2020].
[75] The White House (1 February 2015) National security strategy. Available at: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf [accessed 31 October 2017], p. 4.
[76] Reuters (2 November 2016) Special report – John Brennan's attempt to lead the CIA into the age of cyberwar. Available at: https://uk.reuters.com/article/uk-usa-cia-brennan-specialreport/special-report-john-brennans-attempt-to-lead-the-cia-into-the-age-of-cyberwar-idUKKBN12X1L2 [accessed 11 January 2018].

risk, is a key concern.[77] As Butrimus asserts, the benefits of cyber espionage make it 'too tempting not to use'.[78] The myriad of threats operating in cyberspace are enormous, with the economic costs of cyber espionage estimated to lose the UK £27 billion per year.[79] But the threats are not abating, as former US intelligence chief James Clapper told Congress in 2016, "[cyber] threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact."[80] However, as Clapper acknowledged, of the myriad of threats operating in cyberspace, few, if any, pose as significant a risk as Russia and China.[81]

For decades, Chinese cyber espionage has sustained an enormous campaign of intellectual property theft targeted against the United States and its European partners.[82] As was argued by the FBI's Executive Assistant Director, '[it's] no secret that the Chinese government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries.'[83] According to a US counterintelligence report to Congress, China's mass hacking was driven by a 'longstanding policy of "catching up fast and surpassing" Western powers.'[84] Beijing has been implicated in many highly publicised case of cyber espionage focused against economic targets, such

[77] Butrimas, V. 'National security and international policy challenges in a post *Stuxnet* world', *Lithuanian Annual Strategic Review*, 12, 2014, p. 26
[78] Ibid.
[79] Cabinet Office (November 2011) The UK cyber security strategy. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf [accessed 31 October 2017].
[80] Permanent Select Committee on Intelligence (10 September 2015) World Wide Cyber Threats Hearing. Available at: https://www.youtube.com/watch?v=Q3aG0CtZbU4 [accessed 31 October 2017].
[81] Ibid.
[82] Hughes, R. G. & Chen, K. "The enlightened prince and the wide general': the history of Chinese intelligence', *Intelligence and National Security*, 2018, p. 4; Sims, J. E. 'Democracies and counterintelligence: the enduring challenge', in *Vaults, mirrors & masks: Rediscovering U.S. counterintelligence*, edited by Jennifer E. Sims and Burton Gerber (Washington, Georgetown University Press, 2009), p. 3.
[83] Anderson, R (19 May 2014) Combating state-sponsored cyber espionage, *FBI*, https://www.fbi.gov/news/speeches/combating-state-sponsored-cyber-espionage [accessed 23 February 2018].
[84] Office of the National Counterintelligence Executive (3 November 2011) Foreign spies stealing US economic secrets in cyberspace. Available at: https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf [accessed October 31 2017]. p. 7.

as GhostNET, ShadyRAT, Operation Aurora, and Byzantine Hades.[85] China, however, has long denied such allegations, insisting it does not engage in economic cyber espionage, while accusing the West of hypocrisy in the aftermath of Edward Snowden's disclosures about US technical intelligence gathering.[86]

Despite these objections, the role of the Chinese state was laid bare in the 2013 Mandiant report, a document that attributed a series of sophisticated, persistent, and diverse breaches led by a hacking group designated APT 1 ('advanced persistent threat') to China's People's Liberation Army (PLA) Unit 61388.[87] The report 'revealed evidence directly tying a Chinese military unit to cyber espionage attacks against 141 separate organizations across 20 industries focused almost exclusively in English-speaking countries around the world.'[88] The strength of these allegations was further cemented in the resulting 2014 indictment of PLA Unit 61388 hackers by the US Department of Justice, for 'computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar product industries', a move that reflected Washington's waning tolerance for state-backed economic hacking.[89]

Some hopes arose that Chinese hacking might be perturbed through a 2015 deal between President Obama and President Xi, after the US administration proposed

[85] Applegate, S. 'Cyber conflict: disruption and exploitation in the digital age' in *Current and emerging trends in cyber operations: policy, strategy and practice*, edited by Frederic Lemiuex, (London, Palgrave Macmillan, 2015), p. 29.
[86] Ibid, p. 30; BBC News (23 September 2015) Does China's government hack US companies to steal secrets? Available at: http://www.bbc.co.uk/news/technology-34324252 [accessed 31 October 2017].
[87] Mandiant (February 2013) APT1 Exposing one of China's cyber espionage units. Available at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf [accessed 31 October 2017], p. 59.
[88] Applegate, 'Cyber conflict', p. 29-30.
[89] The United States Department of Justice (19 May 2014) U.S. charges five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization for commercial advantage. Available at: https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor [accessed 31 October 2017]; Applegate, 'Cyber conflict', p. 30.

potential sanctions against Chinese companies who gained from economic theft.[90] As Obama told press, "[we] have agreed that neither the US nor the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage".[91] That same year, an official UK statement declared a similar agreement: '[the] UK and China agree not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information with the intent of providing competitive advantage.'[92] Although many query whether the Obama - Xi agreement could curtail Beijing's hacking ambitions, intelligence officials and cyber security specialists initially reported steep reductions in breaches attributable to China.[93] However, in 2016 the CIA Director (at the time) John Brennan, acknowledged that the deal's long-term effectiveness remained opaque:

> … I do believe that we have seen less incidents of these types of attacks, but I don't know whether or not it is a result of their realising that it's tarnishing their national brand and it is hurting them commercially, politically and economically, or whether or not they are just getting better in terms of being able to hide their fingerprints on this. So I think the jury is still out on it.[94]

Even if the deal is successful, it only applied to economic theft, giving China incentive to shift its extensive hacking resources towards higher valued quarry. As argued by the chief intelligence strategist of security firm FireEye (authors of the Mandiant report):

---

[90] Sevastopulo, D. (22 September 2015) Obama and Xi in deal on cyber espionage, *Financial Times.* Available at: https://www.ft.com/content/0dbcab36-63be-11e5-a28b-50226830d644 [accessed 10 September 2017].
[91] Ibid.
[92] Foreign & Commonwealth Office (22 October 2015) UK – China joint statement on building a global comprehensive strategic partnership for the 21st Century. Available at: https://www.gov.uk/government/news/uk-china-joint-statement-2015 [accessed 31 October 2017].
[93] In 2016 FireEye investigation into China's cyber espionage, sampled incidents attributable to China had reduced from 60-70 a month to around 5, reflecting a 90% reduction. FireEye (21 June 2016) Redline drawn: China recalculates its use of cyber espionage. Available at: https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf [accessed 2 November 2017].
[94] The Aspen Institute (29 July 2016) A candid conversation with the Director of the Central Intelligence Agency, *Youtube*. Available at: https://www.youtube.com/watch?v=TRCUO7-lbUE [accessed 11 January 2018].

"[the] total threat from China didn't decrease, it just changed shape … They've been careful to go after targets where you can't clearly say what they're taking, or where they can defend what they're taking as permissible"[95] Indeed, documents released by Snowden showed that Chinese hackers were highly active against US national security targets prior to the Obama – Xi deal, but reductions in economic hacking may see further action against these more tempting targets:

> Beijing has dramatically expanded its cyber espionage operations in the last five years and has conducted network intrusions … against US military and diplomatic organizations', further adding ''[although] China lags behind Russia in terms of sophistication … the scale and scope of their overall cyber activities and their increasing interest in information associated with NATO and its member states makes them the second most strategic threat to NATO networks.[96]

One often cited case occurred in 2003, when Chinese hackers stole terabytes of information from US defence contractors in an operation dubbed Titan Rain.[97] Most of the information pilfered was sensitive, but not classified, nonetheless the sheer scope of the breach was enough to ramp up concerns.[98] It is, for example, often cited that the hackers stole enough information to fill the entire Library of Congress.[99] But Washington's troubles hit new heights in 2015, when they discovered that Chinese hackers had breached the Office of Personnel Management (OPM).[100] Over 21 million federal government workers were affected by the theft of OPM's sensitive vetting

[95] Greenberg, A. (31 October 2017) China tests the limits of its US hacking truce, *Wired*. Available at: https://www.wired.com/story/china-tests-limits-of-us-hacking-truce/ [accessed 2 October 2017].
[96] Snowden Arcvhive (2 April 2015) NATO Civilian Intelligence Council - Cyber Panel National Input. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0fa7.dir/doc.pdf [accessed 31 October 2017], p.2.
[97] As a Congressional investigation noted, although none of the information was classified, some of it was deemed 'sensitive and subject to U.S. export-control laws'. Wilson, C. CRS report for Congress: Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for Congress, *Congressional Research Service,* 2008. Available at: https://www.fas.org/sgp/crs/terror/RL32114.pdf, [accessed 31 October 2017]. p. 14.
[98] Ibid.
[99] Pool, P. 'War of the cyber world: the law of cyber warfare', *International Lawyer,* 47:2, 2013, p. 306.
[100] Koerner, B. I. (23 October 2016) Inside the cyberattack that shocked the US government, *Wired*. Available at: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ [accessed 1 March 2018].

records, information that could be used to blackmail or recruit vulnerable clearance holders, leading media pundits to describe the incident as the worst breach in American history.[101] While disastrous in its own right, OPM fired a clear signal to US policymakers, that China has the capability, and the willingness, to penetrate some of the most sensitive networks in the federal government.

By comparison, prior to 2014 only a handful of major breaches were tied to the Kremlin, but each case displayed impressive sophistication.[102] One breach of US military classified networks, known as Buckshot Yankee, caused such concern in Washington that it led to the creation of US Cyber Command.[103] By 2014, however, an emboldened Russia began flexing its cyber muscles, releasing a ransomware named Snake into energy and technology sectors across Europe and the US, while expanding operations against NATO members through a group designated APT28.[104] But whereas previously Russian hackers were notoriously difficult to monitor, after 2014 they

[101] Nakashima, E. (21 July 2015) U.S. decides against publicly blaming China for data attack, *The Washington Post.* Available at: https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html?hpid=z1&utm_term=.253069a9fa39 [accessed 2 November 2017]; CNN (24 August 2017) FBI arrests Chinese national connected to malware used in OPM data breach. Available at: http://edition.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html [accessed 2 November 2017].

[102] One leaked US intelligence document states 'Russia is a robust, multi-disciplinary cyber actor with proven access and tradecraft which can conduct the full scope of operations, including computer network exploitation, insider-enabled operations, supply-chain operations, and computer network attack.' For more details, see Snowden Archive (2 April 2015) NATO Civilian Intelligence Council - Cyber Panel National Input. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0fa7.dir/doc.pdf [accessed 31 October 2017], p.1-2; Applegate, 'Cyber conflict', p. 29.

[103] Zetter, K. (9 December 2011) The return of the worm that ate the Pentagon, *Wired*. Available at: https://www.wired.com/2011/12/worm-pentagon/ [accessed 31 November 2017].

[104] Applegate, 'Cyber conflict', p. 29; Sanger, D. E. & Erlanger, S. (March 82014) Suspicion falls on Russia as 'Snake' cyberattacks target Ukraine's government, *The New York Times.* Available at: https://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html [accessed 31 November 2017]; Der Spiegel (May 3 2018) cyber-espionage hits Berlin: the breach from the East. Available at: http://www.spiegel.de/international/germany/cyber-espionage-likely-from-russia-targets-german-government-a-1196520.html [accessed 5 March 2018]; Jones, S. (7 August 2014) Ukraine PM's office hit by cyber attack linked to Russia, *Financial Times.* Available at: https://www.ft.com/content/2352681e-1e55-11e4-9513-00144feabdc0 [accessed 31 November 2017]; FireEye (27 October 2014) APT28: A window into Russia's cyber espionage operations? Available at: https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html [accessed 31 November 2017].

seemed to grandstand on their activities, taking little precautions to mask their tracks.[105] Such shifts were reflected in a 2016 US intelligence report, 'Russia is assuming a more assertive cyber posture based on its willingness to target critical infrastructure systems and conduct espionage operations even when detected and under increased public scrutiny.'[106] This 'critical infrastructure' dimension reflects concerns about Russia's use of cyberspace for aggression, not just intelligence gathering.[107] In 2007, Kremlin hackers caused chaos during Estonian riots by shutting down banks, media outlets and government websites through a series of hacks.[108] And in recent years, Russian hackers have been implicated in a series of cyber-attacks against NATO member states, including causing physical damage to a German steel mill, disabling Finnish Ministry of Defense websites (after a NATO exercise in Finland), and knocking the French television network, TV5 Monde, offline for 18 hours.[109]

Further, concerns about Russian cyber aggression have increased in recent years due to events in Ukraine, where Kremlin hackers have initiated a campaign of sophisticated cyber-attacks.[110] For example, the 2015 Prykarpattyaoblenergo power distribution company hack shut down power for over 200,000 Ukrainians, and is one of

[105] Financial Times (11 January 2017) The changing face of Russian cyber espionage. Available at: https://www.ft.com/content/ea9f93fc-b721-4783-aa7a-d88b3e4e2042 [accessed 31 November 2017].
[106] Office of the Director of National Intelligence (9 February 2016) Worldwide threat assessment of the US intelligence community. Available at: https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf [accessed 31 November 2017]. p. 3.
[107] Prior to 2014, the odds of Russia committing a cyber-attack against a peacetime NATO member were considered very low. As one leaked 2011 US intelligence document states 'We judge that cyber attacks against NATO networks by most nation states, including Russia and China, are unlikely outside of the context of a diplomatic or military conflict. However, we are concerned that the access that adversaries gain from cyber espionage activities could accelerate the deployment of cyber attacks in the event of such a conflict.' For more details, see Snowden Archive (2 April 2015) NATO Civilian Intelligence Council - Cyber Panel National Input. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0fa7.dir/doc.pdf [accessed 31 October 2017], p.1.
[108] BBC News (27 April 2017) How a cyber attack transformed Estonia. Available at: http://www.bbc.co.uk/news/39655415 [accessed 31 November 2017].
[109] The Daily Dot (29 February 2016) Russia's rise to cyberwar superpower. Available at: http://www.dailydot.com/layer8/russia-cyberwar-cyberattack-dnc-breach-history/ [accessed 31 November 2017].
[110] ICS-CERT (25 February 2016) Cyber-attack against Ukrainian critical infrastructure. Available at: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 [accessed 31 November 2017].

many subsequent attacks on Ukrainian critical systems.[111] Passively hacking critical infrastructure is hardly uncommon amongst major cyber actors, both Russia and China have been implicated in the past for infiltrating and mapping US electrical grids.[112] However, Russia's alleged willingness to infiltrate and damage Ukrainian systems raise concerns that it is exploiting the Ukraine as a testing ground for cyber weapons that might be wielded against other nation-states, even in peacetime.[113] As one former intelligence and security official argued, "[that an] adversary that had already targeted American energy utilities had crossed the line and taken down a power grid … [poses] an imminent threat to the United States."[114] Perhaps due to fearing reciprocal action by two established cyber powers, Russia has shied away from serious cyber-attacks against US or UK infrastructure, but it has proven more than prepared to use hacking as a limited form of covert action.[115]

This was underscored through the 2016 Democratic National Committee (DNC) hack, which saw thousands of emails leaked to the press in an act that is thought to have damaged Hillary Clinton's electoral chances.[116] As US intelligence reported, "[we] believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities".[117] It underscored the point that Russia was prepared to use its vast cyber resources to support its political

[111] Zetter, K. (3 March 2016) Inside the cunning, unprecedented hack of Ukraine's power grid, *Wired*. Available at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ [accessed 31 November 2017].
[112] Stoddart, K. 'Live free or die hard: U.S.-UK cybersecurity policies.' *Political Science Quarterly*, 131:4, 2016, p. 812.
[113] Greenberg, A. (20 June 2017) How an entire nation became Russia's test lab for cyberwar, *Wired*. Available at: https://www.wired.com/story/russian-hackers-attack-ukraine/ [accessed 31 November 2017].
[114] Ibid.
[115] CNN (27 June 2017) How one typo helped let Russian hackers in. Available at: http://edition.cnn.com/2017/06/27/politics/russia-dnc-hacking-csr/index.html [accessed 31 November 2017]
[116] BBC News (7 October 2016) US accuses Russia of cyber attacks. Available at: http://www.bbc.co.uk/news/election-us-2016-37592684 [accessed 31 November 2017].
[117] Ibid.

objectives, as Brennan told *CBS News*, "I think that we have to be very, very wary of what the Russians might be trying to do in terms of collecting information in a cyber-realm, as well as what they might want to do with it."[118] Later intelligence reports found that the DNC hack was part of a far wider influence campaign, which included propaganda and narrative manipulation through social media, and Russia's state-sponsored RT News.[119] Similar incidents occurred in France, as Russian hackers tried, but failed, to influence the 2017 election of Emmanuel Macron, further underscoring the brazenness of the Kremlin's cyber power.[120]

In addition to Russian and Chinese cyber threats, human intelligence is a growing area of concern. Modern Chinese espionage is often seen to rely on the "thousand grains of sand" philosophy, whereby it recruits as many spies as possible, usually in economic sectors, in the hope that a fraction of these will provide fruitful results.[121] Further to this view, most of those agents are seen to be Chinese expatriates, who are often recruited by appealing to a common desire for the home nation's prosperity.[122] "It is a fact of life...that China often tries to enlist Ethnic Chinese in its intelligence efforts", stated a joint CIA/FBI report to Congress in 1999, "[when] approaching an individual of Chinese origin, the Chinese intelligence services attempt

[118] CBS News (11 September 2016) 9/11: Nunes, Salvanto, Brennan. Available at: https://www.cbsnews.com/videos/911-nunes-salvanto-brennan/ [accessed 31 November 2017].
[119] Office of the Director of National Intelligence (6 January 2017) Background to "Assessing Russian activities and intentions in recent US elections": The analytical process and cyber incident attribution." Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf [accessed 31 November 2017]. p. 1-4.
[120] BBC News (25 April 2017) Russian hackers 'target' presidential candidate Macron. Available at: https://www.bbc.co.uk/news/technology-39705062 [accessed 23 January 2020].
[121] Hannas, W. C, Mulvenon, J. & Puglisi, A. B. *Chinese industrial espionage: technology acquisition and military modernization,* (London, Routledge, 2013), p. 189; Eftimiades, N. 'China', in *Routledge Companion to Intelligence Studies,* edited by Rovert Dover, Michael S. Goodman, and Claudia Hillebrand (London, Routledge, 2014), p. 93; Interagency OPSEC support staff (2004) Intelligence Threat Handbook, *Federation of American Scientists.* Available at: http://fas.org/irp/threat/handbook/ [accessed 20 August 2016]. p. 22.
[122] Wise, D. *Tiger Trap: America's secret spy war with China*, (Boston, Houghton Mifflin Harcourt, 2011), p. 17.

to secure his or cooperation by playing on this shared ancestry."[123] Although this understanding of Chinese spying centres on scale rather than scope, Beijing is beginning to flex its espionage muscles, pursuing higher valued quarry and sources who are not of Chinese ethnicity.[124] In 2016, US Congress expressed serious concerns about China's increasingly ambitious HUMINT, citing the data stolen in the OPM hack as a major source of vulnerability.[125] As one senator lamented, Chinese hackers had essentially stolen the "largest spy-recruiting database in history".[126]

The Kremlin, by contrast, has gradually escalated espionage against the West since the dissolution of the KGB in 1991. By 2007 Russia held an 'intelligence presence in the United States equal to its Cold War level … presumably indicative of the return on investment.'[127] As of 2016, officials estimated that over 150 Russian operatives were working on American soil, in Washington, New York, and other major cities.[128] In 2010, MI5 claimed Russia's presence in the United Kingdom had also reached Cold War levels, while former GCHQ chief David Omand described their activities as "very active" and "very ruthless".[129] To an extent, this is unsurprising,

[123] Ibid.
[124] Mattis, p. 'The Analytic challenge of understanding Chinese intelligence services', *Studies in Intelligence, CIA*, 56:3, 2012, p. 49-51.
[125] US- China Economic and Security Review Commission (16 November 2016) Section 3: Chinese intelligence services and espionage threats to the United States. Available at: https://www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%202%2C%20Section%203%20-%20China%27s%20Intelligence%20Services%20and%20Espionage%20Threats%20to%20the%20United%20States.pdf [accessed 31 November 2017], p. 292.
[126] Finklea, K. et al. Cyber intrusion into U.S. Office of Personnel Management: In brief. *Congressional Research Service,* 2015. Available at: https://fas.org/sgp/crs/natsec/R44111.pdf [accessed 31 November 2017], p. 4.
[127] Van Cleave, M. 'Strategic counterintelligence: what is it and what should we do about it?' *Studies in Intelligence,* 51:2, 2006, p. 5.
[128] Miller, G. (14 September 2016) As Russia reasserts itself, U.S. intelligence agencies focus anew on the Kremlin, *The Washington Post.* Available at: https://www.washingtonpost.com/world/national-security/as-russia-reasserts-itself-us-intelligence-agencies-focus-anew-on-the-kremlin/2016/09/14/cc212c62-78f0-11e6-ac8e-cf8e0dd91dc7_story.html?postshare=371473956824384&tid=ss_tw-bottom&utm_term=.d8941ad4f02e#comments [accessed 31 November 2017].
[129] Norton-Taylor, R. (29 June 2010) Russian spies in UK 'at cold war levels', says MI5, *The Guardian.* Available at: https://www.theguardian.com/world/2010/jun/29/russian-spies-cold-war-levels [accessed 31 November 2017].

given that Putin's intelligence agencies adopted many of the skills, doctrines, and personnel from the KGB.[130] But with its KGB legacy, the scale of Russia's intelligence presence is only matched by its scope, '[the] general consensus within European counterintelligence services appears to be that Russian collection operations are not just highly active but also often extremely professional'. [131] The SVR, Russia's main espionage agency, entered the public spotlight in 2010, when the FBI announced the arrest of ten Russian 'Illegals', including Anna Chapman and Mikhail Semenko.[132] Early reports lambasted the group for their apparent amateurism, but experts have noted that the case showed Russia was still willing to invest considerable time and resources into establishing its foreign intelligence presence.[133]

[130] Anderson, J. 'The HUMINT offensive from Putin's Chekist state', *International Journal of Intelligence and Counterintelligence,* 20:2, 2007, p.269-275.
[131] Galeotti, M. 'Putin's Hydra: inside Russia's intelligence services', *European Council on Foreign Relations,* 2016. Available at: http://www.ecfr.eu/page/-/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf [accessed 31 November 2017], p. 7.
[132] To quote the DNI, 'An illegal is an officer or employee of an intelligence organization who is dispatched abroad and who has no overt connection with the intelligence organization with which he or she is connected or with the government operating that intelligence organization.' For more details, see Office of the National Counterintelligence Executive (2011) Foreign spies stealing US economic secrets in cyberspace. Available at: https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf [accessed October 31 2017], p.5; FBI - Ghost stories: Russian Foreign Intelligence Service (SVR) Illegals. Available at: https://vault.fbi.gov/ghost-stories-russian-foreign-intelligence-service-illegals [accessed 31 November 2017].
[133] As one Guardian journalist stated '[the tradecraft used by the alleged SVR ring was amateurish, and will send shivers down the spine of the rival intelligence organisations in Russia. This was bungling on a truly epic scale'. For more details, see Hearst, D. (29 June 2010) 'Russian spies' bungle was epic, *The Guardian.* Available at: https://www.theguardian.com/commentisfree/2010/jun/29/russian-spies-bungle-epic [accessed 31 November 2017]; BBC News (29 June 2010) Long history of deep-cover 'illegals'. Available at: http://www.bbc.co.uk/news/10452384 [accessed 31 November 2017]; Lucas, E. *Deception: Spies, lies, and how Russia dupes the West,* (London, Bloomsbury Publishing PLC, 2013), p. 136.

Figure 1: The Russian Illegals arrested in 2010.[134]

Running parallel to these more conventional operations is Russia's use of HUMINT for 'active measures', a legacy from the Soviet disposition for subversion and assassination.[135] Russian intelligence officers have been accused of numerous targeted killings, as emphasised by the assassination of the FSB defector Alexander Litvinenko, allegedly by ex-KGB Andrei Lugovoi.[136] Such aggression is attributed to the fact that Russian intelligence services 'regard themselves as already at war, and operate accordingly'.[137] The 2018 attempted murder of Sergei and Yulia Skripal in Salisbury, UK - which despite being bungled led to the poisoning of numerous uninvolved parties, including the death of Dawn Sturgess – only underscored Russia's

[134] ABC News (7 March 2018) Sergei Skripal: the story behind the Russian double agent found poisoned on a bench in an English town. Available at: https://www.abc.net.au/news/2018-03-07/sergei-skripal-and-anna-chapman-what-we-know/9523970 [accessed 15 January 2021].
[135] Galeotti, 'Putin's Hydra', p. 7.
[136] BBC News (21 January 2016) Alexander Litvinenko: profile of murdered Russian spy. Available at: http://www.bbc.co.uk/news/uk-19647226 [accessed 31 November 2017].
[137] Galeotti, M. (12 May 2017) Russian intelligence is at war, *NATO Review*. Available at: https://www.nato.int/docu/review/articles/2017/05/12/russian-intelligence-is-at-political-war/index.html [accessed 12 September 2020].

continued willingness to run active measures on British and American soil.[138] Russian intelligence officers also played a key role in 2016's US election interference, as the US intelligence community acknowledged: 'Russia, like its Soviet predecessor, has a history of conducting covert influence campaigns focused on US presidential elections that have used intelligence officers and agents and press placements to disparage candidates perceived as hostile to the Kremlin.'[139] The hand of Russian intelligence became clear after former GRU intelligence officer, turned Kremlin lobbyist, Rinat Akhmetshin, met with senior aides to President Trump.[140] Far more severe allegations were levied in allegations by former SIS officer Christopher Steele, including the unproven claim that President Trump had been compromised and blackmailed by the FSB.[141] The serious attention given to the notion that the US President (and those close to him) may have colluded with Putin's regime, as explored in Robert Mueller's investigations into election interference, only underscores the perceived outreach of Russia's foreign operatives.[142]

---

[138] BBC News (8 October 2018) Russian spy poisoning: what we know so far. Available at: https://www.bbc.co.uk/news/uk-43315636 [accessed 20 October 2018].

[139] Office of the Director of National Intelligence (6 January 2017) Background to "Assessing Russian activities and intentions in recent US elections": The analytical process and cyber incident attribution." Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf [accessed 31 November 2017], p. ii.

[140] Reuters (14 July 2017) Russian – American lobbyist met with Trump Jr., Russian lawyer: NBC News. Available at: https://www.reuters.com/article/us-usa-trump-russia-agent/russian-american-lobbyist-met-with-trump-jr-russian-lawyer-nbc-news-idUSKBN19Z189 [accessed 31 November 2017].

[141] The whistleblowing organisation *Cryptome* has disclosed an alleged copy of the document. For more details, see Steele, C. (11 January 2017) US Presidential election: Republican candidate Donald Trump's activities in Russia and compromising relationship with the Kremlin, *Cryptome*. Available at: https://cryptome.org/2017/01/Steele-Trump.pdf [accessed 31 November 2017], p. 1; Schindler, J. R. (10 October 2017) The trouble with the Steele dossier, *Observer*. Available at: http://observer.com/2017/10/fact-versus-fiction-in-the-steele-dossier-on-donald-trump/ [accessed 31 November 2017].

[142] CNN reports that the FBI and US intelligence community took the dossier more seriously than they publicly admitted, including meeting Christopher Steele. Furthermore, former SIS chief Richard Dearlove, told BBC Newsnight that "I think there is probably credibility to the content … I wouldn't put it any more forcefully than that." Nevertheless, the credibility of its content has been widely questioned. Former NSA counterintelligence officer John Schindler notes that some of its wilder claims reflect a Russian tendency for absurd deception, or 'kompromat'. For more details, see the following; CNN (25 October 2017) Exclusive: Mueller's team met with Russia dossier author. Available at: https://edition.cnn.com/2017/10/05/politics/special-counsel-russia-dossier-christopher-steele/index.html [accessed 26 Octomber 2017]; Sabur, R. (13 December 2017) 'Dirty dossier' on Donald trump is

The impetus for espionage

Owing to the issues presented here, it is unsurprising that Russia and China are rising up the intelligence agenda. As former SIS chief, John Sawers, told BBC News, the "stability that we had during the Cold War, or the predominance of the West that we had in the decade or two after the Cold War … is now changing … we're going to have to spend more on our defence and our security because the threats are greater".[143] This is not to suggest that either state ever ceased to be intelligence priorities, since according to documents disclosed by Snowden both were in Washington's top three state priorities by 2014.[144] However, it is evident that nation states are now the *primary* concern for policymakers, outranking the (still important) spectre of terrorism which has dominated policy since 2001.[145] In 2018, US Defence Secretary James Mattis formerly announced that "great power competition, not terrorism, is now the primary focus of US national security", further adding:

> "the American people, the military required to protect our way of life, stand with our allies, and live up to our responsibilities to pass intact, to the next generation, those freedoms that all of us enjoy here today … We face growing threats from revisionist powers, as different as China and Russia are from each

probably credible, says former MI6 boss, *The Telegraph.* Available at http://www.telegraph.co.uk/news/2017/12/13/dirty-dossier-donald-trump-probably-credible-says-former-mi6/?utm_campaign=Echobox&utm_medium=Social&utm_source=Facebook [accessed 10 January 2018]; Higgins, A. & Kramer, A. E. (11 January 2017) Russia's sexual blackmail didn't die with the Soviets, *The New York Times.* Available at: https://www.nytimes.com/2017/01/11/world/europe/donald-trump-russia.html [accessed 10 January 2018]; Schindler, J. R. (11 September 2017) Spies suspect Kremlin is pushing fozens of fake Trump sex tapes, *Observer.* Available at: http://observer.com/2017/11/spy-circles-suspect-kremlin-is-behind-dozens-of-fake-trump-sex-tapes/ [accessed 10 January 2018]; Greenberg, A. (11 January 2017) How spy agency vets read that bombshell Trump report: with caution, *Wired*. Available at: https://www.wired.com/2017/01/spy-agency-vets-read-bombshell-trump-report-caution/ [accessed 31 November 2017].

[143] BBC News (28 February 2015) Sir John Sawers, ex-MI6 chief, warns of Russia 'danger'. Available at: http://www.bbc.co.uk/news/uk-31669195 [accessed 31 November 2017].

[144] Miller, G. (14 September 2016) As Russia reasserts itself, U.S. intelligence agencies focus anew on the Kremlin, *The Washington Post.* Available at: https://www.washingtonpost.com/world/national-security/as-russia-reasserts-itself-us-intelligence-agencies-focus-anew-on-the-kremlin/2016/09/14/cc212c62-78f0-11e6-ac8e-cf8e0dd91dc7_story.html?postshare=371473956824384&tid=ss_tw-bottom&utm_term=.d8941ad4f02e#comments [accessed 31 November 2017].

[145] BBC News (19 January 2018) Mattis: US national security focus no longer terrorism. Available at: https://www.bbc.co.uk/news/world-us-canada-42752298 [accessed 3 February 2018].

> other. Nations that do seek to create a world consistent with their authoritarian models, pursuing veto authority over other nations' economic, diplomatic, and security decisions."[146]

The Defence Secretary's powerful remarks echoed the White House's 2017 National Security Strategy, which placed strenuous emphasis on these "revisionist powers". [147] Similarly, the UK warned of the 'resurgence of state based threats' in its 2015 National Security Strategy, while the SIS chief, Alex Younger, told NATO ambassadors that Russia "exemplified" modern threats facing the UK and its allies.[148] According to media reports, in 2017 British intelligence reclassified Russia as a "tier one" threat, pitting it on at least equal footing to transnational terrorism.[149] Thus, although terrorism will remain a high priority, a security turning point has been reached, carrying major implications for British and American intelligence.

It is clear that understanding Russian and Chinese intentions and capabilities is critical to maintaining peace, avoiding escalation, and ensuring strategic superiority. Espionage may be a means to address this issue, but given the dangers it poses to those who spy, it should be reserved as a method of last resort.[150] As noted by the CIA, 'with inherent risks to human lives', it should 'be preserved for intelligence requirements for which no other collection method exists'.[151] In most cases, the information

---

[146] Ibid.
[147] The White House (December 2017) National Security Strategy. Available at: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf [accessed 2 December 2018], p. 25.
[148] Lucas, E. (1 December 2018) MI6 lays bare the growing Russian threat, *The Times*. Available at: https://www.thetimes.co.uk/edition/comment/mi6-lays-bare-the-growing-russian-threat-sg6vcvl22 [accessed 10 January 2018]; HM Government (November 2015) National security strategy and strategic defence and security review 2015, available at:https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf [accessed 31 October 2017], p. 18.
[149] Business Insider (3 December 2017) British security services are vastly outgunned by the Russian counterintelligence threat. Available at: http://uk.businessinsider.com/british-security-services-vs-russian-counterintelligence-threat-2017-12 [accessed 10 January 2018].
[150] CIA (2013) INTelligence: human intelligence. Available at: https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-human-intelligence.html [accessed 1 January 2017].
[151] Ibid.

policymakers need to know can be gathered through lower risk OSINT or TECHINT, leaving human sources for the remaining gaps.[152] However, the difficulty of collecting intelligence was pinpointed by Victor Madeira while giving evidence on Russian threats to the UK's *Defence Committee* in 2016, wherein he described Moscow and Beijing as taking a strategic approach to protecting their secrets:

> With the end of the Soviet Union, and particularly since 9/11, NATO countries have downgraded, underfunded or outright neglected their counter-intelligence (CI) and counterespionage (CE) functions … Yet strategic rivals such as Russia, China and Iran … regard their 'strategic' approach to CI as crucial in advancing their long-term interests.[153]

This strategic secrecy presents a swathe of issues for lower risk forms of collection, which in turn leads to a wider intelligence gap that must be addressed by human sources. This is a point that is particularly acute when it comes to the matter of open source intelligence, or OSINT. In most cases, open sources provide a substantial amount of information, a point underscored by Randall Forte, a former assistant secretary of state for intelligence and research:

> The rise of information searches and data aggregators like Google has led to a world where 90 percent or more of information out there is available from open sources. This dramatically restricts the areas in which clandestinely acquired intelligence is actually value-added and places the intelligence community in competition with open-sources information. Why spend a billion dollars on a collection program that may deliver the same information as can be had for free on the Internet, only slower and with greater risks? [154]

The benefits of OSINT – including offshoots such as 'social media intelligence (or SOCMINT) – is that it reduces dependency on riskier methods by filling a large amount

[152] Althoff, M. 'Human intelligence', in *The five disciplines of intelligence collection*, edited by Mark M. Lowenthal &Robert M. Clark (Thousand Oaks, CQ Press, 2016), p. 45.
[153] Parliament (25 March 2016) Supplementary written evidence submitted by Dr Victor Madeira. Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/russia-implications-for-uk-defence-and-security/written/31103.pdf [accessed 10 January 2018], p.2.
[154] Devine, J & Loeb, V. *Good hunting: An American spymaster's story,* (New York, Picador, 2014), p. 287.

of gaps .[155] Indeed, even secretive states are not immune to OSINT, as exemplified by Bellingcat's detailed investigations of Russia's 'Little Green Men' fighting in Crimea, or the downing of the passenger flight MH-17 over Ukraine by a Russian surface-to-air missile launcher.[156] That being said, the effectiveness of OSINT is limited against states who tightly control the free flow of information, '[many] governments and other political organisations have programs to manipulate what appears in the public domain'.[157] This is notably true for authoritarian regimes, which often boast extensive powers to censor both Internet and media content.[158]

According to Kringen, Russia boasts aggressive programs 'to misrepresent its activities and intentions and plant false rumors around the world'.[159] Media manipulation is ingrained into Russian political psyche, with the term "political technologies" reflecting Russia's 'instrumental' approach to censorship, '[this] term is widely being used in the Russian media and strangely enough only bears negative connotations when it is applied to 'the Western political technologies' (or 'technologists') in order to justify Russian propagandist response.'[160] The extent of misinformation extends far beyond traditional news media, including so-called Internet

[155] Gioe, D. V. 'The more things change': HUMINT in the cyber age', in *The Palgrave Handbook of Security, Risk and Intelligence,* edited by Robert Dover, Huw Dylan, and Michael Goodman (Palgrave, Macmillan, 2017), p. 215-216.
[156] Bellingcat (13 November 2015) Artillerymen of Russia's 136th Motorized Infantry Brigade in the Donbass. Available at: https://www.bellingcat.com/news/uk-and-europe/2015/11/13/136-brigade-in-donbass/ [accessed 25 October 2019]; Bellingcat (19 June 2019) Identifying the separatists linked to the downing of MH17. Available at: https://www.bellingcat.com/news/uk-and-europe/2019/06/19/identifying-the-separatists-linked-to-the-downing-of-mh17/ [accessed 25 October 2019].
[157] Kringen, J. A. 'Keeping watch on the world: rethinking the concept of global coverage in the US Intelligence Community, *Studies in intelligence, CIA,* 59:3, 2015, p.6
[158] Freedom House (1 November 2017) Freedom of the press 2017, China. Available at: https://freedomhouse.org/report/freedom-press/2017/china [accessed 10 January 2018]; Reporters Without Borders – Russia: Stifling atmosphere for independent journalists. Available at: https://rsf.org/en/russia [accessed 10 January 2018].
[159] Kringen, 'Keeping watch on the world', p. 6.
[160] Morozova, O. 'Russian politics and deception: The Kremlin's reaction to the revolutions of 2004-2014 and information warfare in Russia-Ukraine relations, *MA Russian and Eurasian Studies, Leiden University*, 2017, p.20.

'troll factories' which disseminate false information and sway public narratives on social media. [161] Beijing follows a similar model, '[the] Chinese government has long been suspected of hiring as many as 2 million people to surreptitiously insert huge numbers of pseudonymous and other deceptive writings into the stream of real social media posts', most of which intends to distract citizens from controversial subjects.[162] As added by China analyst, Helen Gao, Beijing is highly adept at shaping public narratives to quell anxieties and suppress dissent.[163]

Thus intelligence must pierce through this pre-packaged reality, but the alternatives to espionage are limited. Imagery satellites, electronic eavesdropping, and even cyber espionage have abundant uses, but they are not a complete substitute for clandestine human sources, as Grey contends:

> …snippets of bugged conversations, intercepted emails or stolen digital files can take you only so far. They are usually meaningless without context. If Putin is heard to say, 'Let's invade Ukraine' or 'Let's kill Obama,' does he really mean it? … Human beings can provide the cultural context that allows you to judge if what someone says needs to be taken seriously, together with background knowledge about their ambitions, friends and enemies.[164]

Context is one of espionage most important benefits, a 'well-placed asset might be in a position to pose the question to a foreign leader: "What will you do if the United States does X?", giving HUMINT a unique ability to, as former CIA officer John Millis adds, "shake the intelligence apple from the tree, where other intelligence collection techniques must wait for the apple to fall."[165] As further argued by the former Inspector

---

[161] CNN (17 October 2017) Exclusive: Putin's 'chef,' the man behind the troll factory. Available at http://edition.cnn.com/2017/10/17/politics/russian-oligarch-putin-chef-troll-factory/index.html [accessed 10 January 2018].
[162] King, Pan, & Roberts, 'How the Chinese government fabricates social media posts for strategic deception, not engaged argument', *American Political Science Review,* 111:3, 2017, p. 484.
[163] Gao, H. (2 February 2015) China sharpens its censorship blade, *The New York Times.* Available at: https://www.nytimes.com/2015/02/03/opinion/china-sharpens-its-censorship-blade.html?_r=0 [accessed 10 January 2018].
[164] Grey, S. *The new spymasters: inside espionage from the Cold War to global terror,* (New York, Viking, 2015), p. 286.
[165] Johnson, L. K. *National security intelligence: secret operations in defense of the democracies,* (Cambridge, Polity, 2012), p. 48

General of the CIA, Frederick Hitz, '[confirming] and amplifying information acquired by other means is often the role [HUMINT] information plays best'.[166] Similar sentiments are expressed by former SIS officer Nigel Inkster, who notes that despite the advantages offered by technical intelligence, the most important secrets are not written on paper, but 'remain in the minds of people'. [167]

In addition to adding context, it is also becoming harder to perform certain forms of TECHINT, owing to the disclosures of Edward Snowden, who exposed NSA operations to the general public (and US competitors), a point expressed by the CIA's former Deputy Director, David S. Cohen:

> … largely because of unauthorised disclosures revealing how the US Intelligence Community conducts signals intelligence, some of our most potent and dangerous adversaries – state and non-state actors alike – have become savvier in thwarting technical methods of collection. As Director of National Intelligence Jim Clapper recently said, these unauthorized disclosures have "done huge damage for our collection … make no mistake about it." That loss of collection puts even more of a premium on HUMINT.[168]

There is, for example, a strong belief within British intelligence that Russia and China had deciphered the cache of files that Snowden had not released to the public.[169] If the allegations are true, then the loss would represent, as former GCHQ chief David Omand argues, a "huge strategic setback", for 'Britain, America, and their NATO allies.'[170] But even Snowden's public disclosures carried lasting effects, mainly by revealing the extent to which mainstream Internet companies cooperated with British

---

[166] Hitz, F. P. *The great game: the myths and reality of espionage,* [Kindle version] (New York, Vintage, 2005), p. 91
[167] Inkster, N. 'Intelligence agencies and the cyber world', *Strategic Survey*, (2012), p. 47.
[168] CIA (8 September 2015) Deputy Director Cohen delivers remarks on CIA of the future at Cornell University. Available at: https://www.cia.gov/news-information/speeches-testimony/2015-speeches-testimony/deputy-director-cohen-delivers-remarks-on-cia-of-the-future-at-cornell-university.html [accessed 10 January 2018]
[169] Harper, T. (14 June 2015) British spies betrayed to Russians and Chinese, *The Times.* Available at: https://www.thetimes.co.uk/article/british-spies-betrayed-to-russians-and-chinese-xxj7zx5n83d [accessed 22 November 2016].
[170] Ibid.

and American intelligence services.[171] The PRISM programme, for example, showed that mainstream companies were providing customer data directly to the NSA and GCHQ.[172] Consequently, there is growing consensus among governments, including Russia and China, to contain Internet data within localised servers, beyond the legal jurisdiction of Western governments.[173] If Facebook stores its Russian customers' data in a Russian server, neither British nor American intelligence can demand access to that information.[174] Even in the case were communications can be intercepted, modern encryption standards are practically (outside of rare exceptions) unbreakable.[175] Adding to this problem, China is in the process of rolling out 'quantum communications', that are allegedly impervious to eavesdropping (intercepting a quantum communication in transit leaves a particle trace, allowing the sender and receiver to know if a communication has been interrupted in some way).[176]

In addition, although cyber espionage offers opportunities, it also carries severe limitations where the highest valued secrets are concerned. The NSA's advance hacking division, known as Tailored Access Operations, 'has reportedly been one of the most successful units at NSA post-9/11 by producing valuable intelligence on targets ranging from high-level nation-state rivals to counterterrorism targets'.[177] By 2013 a

[171] The Guardian (7 June 2013) NSA Prism program taps in to use data of Apple, Google and others. Available at: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [accessed 3 February 2014].
[172] Ibid
[173] Selby, J 'Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?', *International Journal of Law and Information Technology,* 25:3, 2017, p. 213-215.
[174] Ibid.
[175] The US government and military, as a case in point, use AES-256 encryption, which, even with a super computer, would require billions of years of processing time to decipher (by current computing standards). For more information, see Simms – Levels of encryption. Available at: https://www.simms.co.uk/tech-talk-2/levels-of-encryption/ [accessed 10 January 2018]; Barrett, B. (7 March 2017) Don't let WikiLeaks scare you off of Signal and other encrypted chat apps, *Wired*. Available at: https://www.wired.com/2017/03/WikiLeaks-cia-hack-signal-encrypted-chat-apps/ [accessed 10 January 2018].
[176] BBC News (24 July 2017) China set to launch an 'unhackable' internet communication. Available at: http://www.bbc.co.uk/news/world-asia-40565722 [accessed 10 January 2018].
[177] Loleski, S. 'From cold to cyber warriors: the origins and expansion of NSA's Tailored Access Operations (TAO) to Shadow Brokers', *Intelligence and National Security,* 34:1, 2018, p. 119-120.

joint operation between the NSA and Sweden's SIGINT agency, the FRA, had already gained access to high-level intelligence on Russia's leadership and internal politics.[178] That same year, *Foreign Policy* reported that the NSA had 'successfully penetrated Chinese computer and telecommunications systems for almost 15 years, generating some of the best and most reliable intelligence … about what is going on inside the People's Republic of China.'[179] But despite these successes, classified networks are generally disconnected from the Internet, meaning hackers often require a human source to bridge the gap.[180] As Corera argues, '[the] saving grace for the old human spies was that access to the hardest targets still often required a human agent', adding 'MI6 might become the enabler of GCHQ cyber espionage operations by providing the human access point into a network.'[181] In fact, according to Snowden's disclosures GCHQ runs 'HUMINT Operations Teams' (Hot) for "identifying, recruiting, and running covert agents in the global telecommunications industry"[182] Meaning, as Duvenage and Solms claim, 'success in the field of [cyber intelligence] thus depended on the effectiveness of HUMINT operations.'[183] According to former CIA officer Henry Crumpton, the US intelligence community accepted this reality by the 1990s, with the CIA even setting up a *Clandestine Information Technology Office* (CITO) in

[178] Snowden Archive (2013) (S//REL to USA, FVEY) Subject: NSA intelligence relationship with Sweden, *Snowden Archive*. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH9385.dir/doc.pdf [accessed 10 January 2018].
[179] Aid, M. M. (2013) Inside the NSA's ultra-secret China hacking group, *Foreign Policy.* Available at: http://foreignpolicy.com/2013/06/10/inside-the-nsas-ultra-secret-china-hacking-group/ [accessed 10 January 2018].
[180] Rid, T. *Cyber war will not take place,* (Oxford, Oxford University Press, 2013), p. 81-112.
[181] Corera, G. *Intercept: the secret history of computers and spies,* [Kindle version] (London, Weidenfeld & Nicolson, 2015). Accessed 10 January 2018, p. 343-4.
[182] Ball, J. et al. (6 September 2013) Revealed: how US and UK spy agencies defeat internet privacy and security, *The Guardian.* Available at: https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [accessed 10 January 2018].
[183] Duvenage, P. & Solms, S. 'Putting counterintelligence in cyber counterintelligence: back to the future', *Proceedings of the 13th European Conference on Cyber Warfare and Security*, edited by Andrew Liaropoulos and George Tsihrintzis, (Reading, Academic Conferences and Publishing International Limited, 2014), p. 72-73.

partnership with the NSA, which emphasised human sources as the pathway towards collecting 'terabytes of intelligence booty.' [184]

The issues raised here also extend to counterintelligence, where espionage still has a key role to play. Faced with a rising tide of cyber threats, the US government invested billions of dollars to strengthen its networks, increasing its cyber security budget by over 35 percent in 2017 alone.[185] Similarly, in 2016 the UK launched a five-year plan to invest an additional £1.9 billion to cyber security, more than doubling its previous expenditure.[186] These measures have also run parallel to security defences aimed directly at key threats, as underscored when Obama's administrations released 'declassified technical information on Russian civilian and military intelligence service cyber activity, to help network defenders in the United States and abroad identify, detect, and disrupt Russia's global campaign of malicious cyber activities.'[187] In a further symbolic move, Trump's administration banned Kaspersky antivirus software (a Russian firm) across all federal agencies, in direct retaliation to accusations that Kaspersky's software was enabling Kremlin hackers. [188] However, as reported by Congress, these security measures, while helpful, are only a surface level deterrence against Russian or Chinese cyber operations:

---

[184] Crumpton, H. A. *The art of intelligence: lessons from a life in the CIA's clandestine service*, (New York, Penguin Books, 2012), p. 79-80.
[185] U.S. – China Economic and Security Review Commission (16 November 2016) Annual report to Congress. Available at: https://www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%202%2C%20Section%203%20-%20China%27s%20Intelligence%20Services%20and%20Espionage%20Threats%20to%20the%20United%20States.pdf [accessed 10 January 2018], p. 301-302.
[186] HM Treasury (17 November 2015) Chancellor's speech to GCHQ on cyber security. Available at: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security [accessed 10 January 2018] .
[187] The White House (29 December 2016) Statement by the President on actions in response to Russian malicious cyber activity and harassment. Available at: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity [accessed 10 January 2018].
[188] Solon, O. (13 September 2017) US government bans agencies from using Kaspersky software over spying fears, *The Guardian.* Available at: https://www.theguardian.com/technology/2017/sep/13/us-government-bans-kaspersky-lab-russian-spying [accessed 10 January 2018].

> Increased cybersecurity measures could mitigate, but will not eliminate, the threat of Chinese cyber espionage. Cyber intruders generally develop new approaches more quickly than their targets can develop defenses. Moreover, the human element of cyber espionage is difficult, and sometimes impossible, to defend against. Poor personal cybersecurity practices and procedures among insiders, as well as intentional leaks by insiders, can aid infiltrators.[189]

In order to tackle sophisticated opponents, governments will need to strengthen their offensive counterintelligence posture, to which espionage will need to a play a key role.[190] The UK government explicitly stated that it is adopting a more offensive strategy, announcing its intent 'towards taking the fight to those who threaten Britain in cyber-space and relentlessly pursuing anyone who persists in attacking us.'[191] Furthermore, according to official sources for the *Washington Post*, Obama's government responded to Russian election interference by ordering the NSA to penetrate Russian networks with a breach of its own:

> The cyber operation is still in its early stages and involves deploying "implants" in Russian networks deemed "important to the adversary and that would cause them pain and discomfort if they were disrupted," a former U.S. official said.
>
> The implants were developed by the NSA and designed so that they could be triggered remotely as part of retaliatory cyber-strike in the face of Russian aggression, whether an attack on a power grid or interference in a future presidential race.[192]

These are intended to send a clear message regarding the NSA's own offensive capability, showing the Kremlin that cyber breaches can work both ways.[193] However,

---

[189] U.S. – China Economic and Security Review Commission (16 November 2016) Annual report to Congress. Available at: https://www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%202%2C%20Section%203%20-%20China%27s%20Intelligence%20Services%20and%20Espionage%20Threats%20to%20the%20United%20States.pdf [accessed 10 January 2018], p. 301-302.

[190] Duvenage, P. et al. 'The cyber counterintelligence process – a conceptual overview and theoretical proposition', *Proceedings of the 14th European Conference on Cyber Warfare & Security*, edited by Nasser Abouzakhar, (Reading, Academic Conferences and Publishing International Limited, 2014), p.50.

[191] Cabinet Office (1 November 2016) Britain's cyber security bolstered by world-class strategy. Available at: https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy [accessed 10 January 2018].

[192] Miller, G. et al. (23 June 2017) Obama's secret struggle to punish Russia for Putin's election assault, *The Washington Post.* Available at: https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.73bfdde12b13 [accessed 10 January 2018].

[193] Ibid.

given the risk of escalation, retaliatory measures require certainty that opposing intelligence agencies have crossed an unacceptable line, a certainty that is hard to find when cyberspace affords offenders deniability.[194] As argued by cybersecurity specialist Ben Buchanan, "[the problem with cybersecurity—because cyber capabilities come out of the intelligence community, come out of the secret world, and indeed because they require secrecy in order to work—is that nations don't have a great understanding of each other's cyber capabilities. It's a counterintelligence issue."[195] Duvenage et al further this argument, noting that effective cyber counterintelligence depends on knowledge of an opponent's cyber 'instrumentalities', thereby requiring intelligence gathered through covert sources. [196]

It is also important to determine the intent behind a breach, as a penetration of a system can carry both offensive and defensive benefits. Misperception is highly common in the realm of hacking, 'the harder it gets to differentiate an offensive intrusion from a defensive intrusion, the more real the cybersecurity dilemma is.'[197] To illustrate, China's motivations for breaching OPM systems remain ambiguous, since the files stolen offered offensive and defensive advantages.[198] One report from the Congressional Research Service noted that '[assumptions] about the nature, origins, extent, and implications of the data breach may change', and that it remained 'unclear

[194] A substantial issue here is the 'attribution problem', and the fact that sophisticated cyber actors copy methods from criminal communities and other states, either to save times, cut costs, or to blur attribution. For more details, see Brenner, *America the vulnerable,* p. 50-51.
[195] Sebenius, A. (28 June 2017) Writing the rules of cyberwar, *The Atlantic.* Available at: https://www.theatlantic.com/international/archive/2017/06/cyberattack-russia-ukraine-hack/531957/ [accessed 10 January 2018].
[196] Duvenage, P. et al. 'The cyber counterintelligence', p. 50.
[197] Sebenius, A. (28 June 2017) Writing the rules of cyberwar, *The Atlantic.* Available at: https://www.theatlantic.com/international/archive/2017/06/cyberattack-russia-ukraine-hack/531957/ [accessed 10 January 2018].
[198] In terms of offensive capabilities, as noted, China may now have abundant information to recruit US government employees for HUMINT. But from a defensive perspective, as is explored in chapter two, the data may be highly valuable for identifying undercover CIA officers. For further details, see CNN (30 September 2015) U. S. pulls spies from China after hack. Available at: http://money.cnn.com/2015/09/30/technology/china-opm-hack-us-spies/index.html [accessed 10 January 2018].

how data from the OPM breaches might be used if they are indeed now in Chinese government hands'[199] Addressing this uncertainty is crucial, given that the Obama administration strongly considered retaliation for a breach that some US politicians felt was unacceptable.[200] When cyber intrusions can incur sanctions, retaliatory strikes, or political uproar, it is even more important to determine both culpability and intent, both of which are likely to be hidden from plain sight

In terms of tackling the threats faced by foreign HUMINT, both the FBI and MI5 continue to substantially invest in protective security, meaning basic security measures designed to impede the activities of spies.[201] But since 2016, diplomatic expulsions have formed a key line of defence, as underscored when the Obama administration declared 35 Russian diplomats persona non grata and shut two diplomatic compounds in Maryland and New York (which were identified as intelligence bases).[202] On this occasion, the Russians did not respond in kind, but when

[199] Finklea, K. et al. Cyber intrusion into U.S. Office of Personnel Management: In brief. *Congressional Research Service*, 2015. Available at: https://fas.org/sgp/crs/natsec/R44111.pdf [accessed 31 November 2017], p. 1-4.

[200] Sanger, D. E. (31 July 2015) U.S. decides to retaliate against China's hacking, *The New York Times.* Available at: https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html [accessed 10 January 2018].

[201] The FBI, as a case in point, has established a significant informational programme to spread awareness of insider threat risks and methods. Similarly, MI5 notes that 18% of its resources are allocated to counter espionage, counter proliferation, and protective security – although the agency clarified to the *Intelligence and Security Committee* that such percentages are misleading, particularly in the resources devoted to Russia, due to substantial staff increases. For more details see FBI – The insider threat: an introduction to detecting and deterring an insider spy. Available at: https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view [accessed 10 January 2018]; Intelligence and Security Committee of Parliament (20 December 2017) Annual report 2016-2017. Available at: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/2016-2017_ISC_AR.pdf?attachauth=ANoY7cplYx6_T2wqvneNY2u1lJGYvVbvNYwc9QwGaR24Ke484uJPSMX8iwoAkHde3Rtk-RJ_K3j5vLNz7TQ16I2XenBmJfy9xj5vQ3-JFAittxF6ITyyHKFG7pu665Ocl8xWd9wpBk-r5q-7UGE8D79HPss8ZQ_s0wm8A5ZK7x8Ca25XqKeOOsMXjFgCComcbWXcwl8UxyNferNQhBZjHUEXoM2gRdkJKL4ZgGH3QNqGoqgeiFaRduA%3D&attredirects=0 [accessed 11 January 2018], p. 49.

[202] The White House (2016) Statement by the President on actions in response to Russian malicious cyber activity and harassment. Available at: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity [accessed 10 January 2018].

[202] CNN (26 March 2018) Trump expelling 60 Russian diplomats in wake of UK nerve agent attack. Available at: https://edition.cnn.com/2018/03/26/politics/us-expel-russian-diplomats/index.html [accessed 3 April 2018]; The White House (29 December 2016) Statement by the President on actions in response to Russian malicious cyber activity and harassment. Available at:

the UK and US government expelled a swathe of Russian diplomats in response for the Salisbury Novichok attack, the Kremlin retaliated with mass expulsions of its own.[203] This was followed by further expulsions under president Trump, with 60 Russian diplomats evicted in response to nerve-agent attacks against the Skripals in the UK, all of whom had been identified as intelligence officers.[204] In the UK, despite alleged efforts to downsize Russia's diplomatic presence by denying individual visas to certain diplomats (as protested by the Russian embassy), the Skripal attacks validated far more robust action.[205] In 2018, the UK government responded by expelling 23 Russian diplomats, despite protests by the Kremlin.[206] Similar actions were seen in 2020, when the shutting of a Chinese consulate in Houston (supposedly for intellectually property theft) led to the shutting of an American consulate in Chengdu.[207] This race to the bottom favours neither side, but owing to the liberal immigration policies of democracies, it is far easier for Russia or Chinese operatives to enter American soil than vice versa.[208] As argued by one former FBI official, "I think it will have a short-term effect on Russian intelligence collection within the United States … the game will

---

https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity [accessed 10 January 2018].

[203] BBC News (14 March 2018) Russian soy: UK to expel 23 Russian diplomats. Available at: https://www.bbc.co.uk/news/uk-43402506 [accessed 20 March 2018]; CNN (16 March 2018) Trump expelling 60 Russian diplomats in wake of UK nerve agent attack. Available at: https://edition.cnn.com/2018/03/26/politics/us-expel-russian-diplomats/index.html [accessed 3 April 2018]; CNN (29 March 2018) Russia expels US diplomats and shuts consulate in tit-for-tat move. Available at: https://edition.cnn.com/2018/03/29/europe/russia-expels-us-diplomats-intl/index.html [accessed 21 November 2019].

[204] CNN (26 March 2018) Trump expelling 60 Russian diplomats in wake of UK nerve agent attack. Available at: https://edition.cnn.com/2018/03/26/politics/us-expel-russian-diplomats/index.html [accessed 3 April 2018].

[205] Independent (22 October 2016) Russian ambassador to UK claims embassy is 'shrinking' because government is delaying staff visas. Available at: http://www.independent.co.uk/news/uk/home-news/russian-ambassador-embassy-shrinking-delay-visas-staff-alexander-yakovenko-foreign-office-a7375171.html [accessed 10 January 2018].

[206] BBC News (14 March 2018) Russian soy: UK to expel 23 Russian diplomats. Available at: https://www.bbc.co.uk/news/uk-43402506 [accessed 20 March 2018].

[207] BBC News (24 July 2020) US consulate: China orders US consulate closure in tit-for-tat move. Available at: https://www.bbc.co.uk/news/world-asia-china-53522640 [accessed 13 September 2020].

[208] Schmidle, N. (7 August 2017) The U.S. has more to lose than Russia in spy expulsions, *The New Yorker.* Available at: https://www.newyorker.com/news/news-desk/the-us-has-more-to-lose-than-russia-in-spy-expulsions [accessed 10 January 2018].

go on … intelligence officers are always replaceable."[209] But the seeming ease by which Russia and China can replace their losses poses serious strains on more effective counterintelligence practices. Surveillance, for instances, is usually considered a key line of defence, but according to one senior US official, the FBI faces a "math problem … It takes a lot of folks to run surveillance on one individual and make sure you never lose contact."[210] This factor is only worsened by globalisation, which enables Russian and Chinese intelligence officers to pursue their targets on foreign soil, in relative privacy from British or American surveillance.[211]

One 'surefire' way to tackle this problem, as Cohen puts it, 'is to collect intelligence on the efforts underway by our adversaries'.[212] But foreign intelligence agencies are the hardest of hard targets, and despite its advantages technical intelligence is mired by limitations.[213] This puts espionage at the forefront of any effective counterintelligence strategy, since if there are no alternative means to penetrate a foreign intelligence agency, then espionage is the last resort, 'the FBI's job and, by extension, Americans' constitutional protections, are strengthened by a more effective

[209] Mazetti, M. & Goldman, A. (30 December 2016) 'The game will go on' as U.S. expels Russian diplomats, *The New York Times.* Available at: https://www.nytimes.com/2016/12/30/us/politics/obama-russian-spies.html [accessed 10 January 2018].
[210] Schmidle, N. (7 August 2017) The U.S. has more to lose than Russia in spy expulsions, *The New Yorker.* Available at: https://www.newyorker.com/news/news-desk/the-us-has-more-to-lose-than-russia-in-spy-expulsions [accessed 10 January 2018].
[211] As the FBI's 2017 fiscal budget notes '[a] particular focus of our counterintelligence efforts are aimed at the growing scope of the insider threat—that is, when trusted employees and contractors use their legitimate access to steal secrets for personal benefit or to benefit another company or country. This threat has been exacerbated in recent years as businesses have become more global and increasingly exposed to foreign intelligence organizations.' For more details, see FBI (27 September 2017) Current threats to the homeland. Available at: https://www.fbi.gov/news/testimony/current-threats-to-the-homeland [accessed 10 January 2018].
[212] CIA (18 September 2015) Deputy Director Cohen delivers remarks on CIA of the future at Cornell University. Available at: https://www.cia.gov/news-information/speeches-testimony/2015-speeches-testimony/deputy-director-cohen-delivers-remarks-on-cia-of-the-future-at-cornell-university.html [accessed 10 January 2018].
[213] As a case in point, Dutch intelligence gathered evidence of Russian election interference by hacking the CCTV cameras in the office of a Russian cyber espionage group known as "Cozy Bear". For more details, see Ars Technica (26 January 2018) Candid camera: Dutch hacked Russians hacking DNC, including security cameras. Available at: https://arstechnica.com/information-technology/2018/01/dutch-intelligence-hacked-video-cameras-in-office-of-russians-who-hacked-dnc/ [accessed 20 January 2020].

CIA.'[214] This, as Cohen adds, 'is classic spy v. spy stuff—and there is no reason to expect that it will abate in the future.'[215] Indeed, Tennent Bagley once claimed that it "takes a mole to catch a mole", but in today's world 'moles' are just as important for addressing cyber threats as they are for uncovering foreign spies.[216] A spy inside the ranks of a Chinese PLA hacking group, as a case in point, could not only confirm Beijing's responsibility behind a breach, but also what they intend to do with the stolen data. In fact, perhaps unsurprisingly, the Kremlin responded to allegations of election interference by arresting several FSB officials for treason, implying that a spy may have aided US intelligence community's assessments.[217]

If espionage is reserved only for filling the most pressing intelligence gaps, for which no other solution exists, then today's spy agencies have an enormous role to play in tackling China's rise and Russian aggression. This was demonstrated in 2016, when, as part of a major investment in its intelligence services, the UK government injected the bulk of its funding into SIS, with its overall staff set to increase by approximately forty percent.[218] Furthermore, according to the 2016-2017 report of the *Intelligence and Security Committee*, SIS now allocates 'around two-thirds of its efforts against nation states' (compared to just under half for GCHQ).[219] Similar signs of change emerged in

---

[214] Sims, J. E. & Gerber, B. 'The way ahead', *Vaults, Mirrors & Masks: Rediscovering U.S. counterintelligence*, edited by Jennifer E. Sims and Burton Gerber, (Washington, Georgetown University Press, 2009), p. 283

[215] CIA (18 September 2015) Deputy Director Cohen delivers remarks on CIA of the future at Cornell University. Available at: https://www.cia.gov/news-information/speeches-testimony/2015-speeches-testimony/deputy-director-cohen-delivers-remarks-on-cia-of-the-future-at-cornell-university.html [accessed 10 January 2018].

[216] Bagley, T. H. *Spy wars: moles, mysteries, and deadly games*. [Kindle version] (New Haven, Yale University Press, 2007). Accessed 1 February 2018, see chapter 13.

[217] Walker, S. (31 January 2017) Russia accuses cybersecurity experts of treasonous links to CIA, *The Guardian.* Available at: https://www.theguardian.com/world/2017/jan/31/russian-cybersecurity-experts-face-treason-charges-cia [accessed 10 January 2018].

[218] BBC News (21 September 2016) MI6 set to recruit 1,000 extra staff. Available at: http://www.bbc.co.uk/news/uk-37434131 [accessed 10 January 2018].

[219] It is also notable that Russia and China are the first two nation states in the document to be listed (followed by Iran, North Korea, and 'other countries'), with Russia receiving almost twice as much commentary as the other states. For more details, see Intelligence and Security Committee of Parliament (20 December 2017) Annual report 2016-2017. Available at:

2017, when Obama's administration transferred responsibility for targeted drone strikes from the CIA to the DoD.[220] The move is interpreted by some specialists as an effort to 'shift the C.I.A.'s focus back toward traditional spying and strategic analysis.'[221] By 2016, Russia accounted for around 10 percent of the CIA's budget, a significantly smaller amount than the 40 percent devoted to the Soviet Union and its allies.[222] But Congress has tried to accelerate the CIA's shift toward nation-state spying, particularly Russia, by 'steering tens of millions of additional dollars toward Russian-related espionage' in the 2015-2016 intelligence budget.[223] Given that these Russian and Chinese threats continue to mount, it is highly likely that the percentage of resources targeted towards them will increase.

Since counterterrorism has dominated intelligence agendas since 9/11, the shift towards more traditional spying will not be easy, as Mark Lowenthal argues "[there's] a huge cultural and generational issue at stake here … A lot of the people hired since 9/11 have done nothing but tactical work for the past 12 years … and intellectually it's very difficult to go from a tactical approach to seeing things more strategically."[224] According to the *New York Times*, there are concerns within the intelligence community about the preparedness of operatives who have spent most of their careers in counterterrorism, 'trying to recruit Russian sources and to outwit Russian

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727949/ISC-Annual-Report-2016-17.pdf [accessed 11 January 2018], p. 49.

[220] Mazetti, M. (24 May 2013) New terror strategy shifts C.I.A, *The New York Times.* Available at: http://www.nytimes.com/2013/05/24/us/politics/plan-would-orient-cia-back-toward-spying.html [accessed 10 January 2018].

[221] Ibid.

[222] Miller, G. (14 September 2016) As Russia reasserts itself, U.S. intelligence agencies focus anew on the Kremlin, *The Washington Post.* Available at: https://www.washingtonpost.com/world/national-security/as-russia-reasserts-itself-us-intelligence-agencies-focus-anew-on-the-kremlin/2016/09/14/cc212c62-78f0-11e6-ac8e-cf8e0dd91dc7_story.html?postshare=371473956824384&tid=ss_tw-bottom&utm_term=.d8941ad4f02e#comments [accessed 31 November 2017].

[223] Ibid.

[224] Mazetti, M. (24 May 2013) New terror strategy shifts C.I.A, *The New York Times.* Available at: http://www.nytimes.com/2013/05/24/us/politics/plan-would-orient-cia-back-toward-spying.html [accessed 10 January 2018].

intelligence officers requires a subtlety that spies have not always practiced in Iraq and Afghanistan.'.[225] Of key concerns, officials worry that it will take a considerable amount of time before most officers are ready to work in Russia, "[it] is a pipeline process … [it] will be years before they can be used operationally."[226] Similar concerns were expressed by Madeira, who described a serious 'lack of relevant language skills in British national security and diplomatic circles'. [227]

Language barriers pose obvious impediments to recruiting spies, but it can take years of classes to gain just a basic grasp of Mandarin, let alone preparing intelligence officers for the dozens of languages used in China.[228] However, American students who have travelled to Russia and China have been routinely targeted by intelligence agencies, meaning Langley is hesitant to recruit candidates who wield the cultural and language skills that make an ideal intelligence officer. Glenn Duffie Shriver is one case in point, who was caught in 2010 trying to apply for a job in the agency despite being recruited by MSS during his studies in China. As one senior CIA officer argues, Shriver gave "the security folks a big concern about the targeting of American students in China … there's a far greater scrutiny of anyone who has spent time in China as a student, particularly on the longer-term programs".[229] Although some in this bracket are still hired if they pass security checks, overall, the CIA's recruitment of more qualified

[225] Ibid.
[226] Miller, G. (14 September 2016) As Russia reasserts itself, U.S. intelligence agencies focus anew on the Kremlin, *The Washington Post.* Available at: https://www.washingtonpost.com/world/national-security/as-russia-reasserts-itself-us-intelligence-agencies-focus-anew-on-the-kremlin/2016/09/14/cc212c62-78f0-11e6-ac8e-cf8e0dd91dc7_story.html?postshare=371473956824384&tid=ss_tw-bottom&utm_term=.d8941ad4f02e#comments [accessed 31 November 2017].
[227] Parliament (25 March 2016) Supplementary written evidence submitted by Dr Victor Madeira. Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/russia-implications-for-uk-defence-and-security/written/31103.pdf [accessed 2 January 2018], p. 7.
[228] Stein, J. (31 March 2017) Why the CIA is increasingly worried about China's moles, *Newsweek*. Available at: http://www.newsweek.com/cia-chinese-moles-beijing-spies-577442 [accessed 10 January 2018].
[229] Ibid.

candidates has stalled. As another officer candidly asserted "[if] you have that on your background, your résumé is just tossed in the trash, because they are so paranoid about MSS penetration and co-opting students".[230] Similar suspicions have spread to applicants with ties to countries such as Iran, Russia, and Eastern Europe, and the implications could be profound, curtailing Langley's access to bilingual candidates, with the skills for Russian and Chinese field work.[231] Therefore, building a work force ready for the hard-target theatres of Moscow and Beijing will require a long-term, culturally transformative process, rather than a seamless transition from decades of counterterrorist operations back to nation states. Nonetheless, as this section has showed, it is a transition that cannot be ignored.

Evaluation

As this chapter has argued, "China's rise and Russian aggression" posits severe implications for Western security, most notably through the serious threat of conventional hostilities. Contrary to early assumptions that the Cold War's ending would bring about a new century of peace and prosperity, friendly relations with Russia and China have proven short lived. In Russia's case, the Kremlin's increasingly authoritarian model of government and perceived containment by NATO, has seen it steadily challenge Western power throughout Eastern Europe and beyond. Its incursions and proxy wars in Georgia and Ukraine demonstrate Putin's willingness to exert influence through military action, while its role in Syria shows it is capable of challenging US power on the world stage. Similarly, China's expansionist ambitions in the Pacific, which are shaped by its own perception of American containment, raise the

[230] Ibid.
[231] Ibid.

prospect of hostility in the East and South China seas. In both cases, the West's response, including bolstering NATO and a strategic pivot to Asia, are only escalating tensions, with Beijing and Moscow strengthening their own hands through ongoing military and nuclear modernisation programmes.

These issues have only been worsened by Russia and China's aggressive and ambitious intelligence activities. One of the gravest concerns is Russia's willingness to use its well-honed intelligence resources to shirk conventional norms. The Salisbury assassination attempt proved to international audiences that its intelligence agencies were still willing to commit murder on foreign soil, while its involvement in 2016 election interference revealed an impressive aptitude for more advanced forms of covert action. Those concerns have only been fuelled by its cyber-attacks against the Ukraine and Estonia, which indicate that the Kremlin is capable of inflicting severe harm on critical infrastructure from afar. Likewise, China's decades long campaign of intellectual property theft and economic espionage has caused billions of dollars' worth of harm to Western businesses. But its involvement in the 2018 Office of Personnel Management hack demonstrated Beijing's readiness to turn its vast intelligence resources towards higher valued quarry, both through technical and human means.

As has been shown, these threats are not merely a blip of declining relations to be fixed through a diplomatic conference, they are long term, slow-building problems that have shown no improvement. While the United States still dominates the international order, it is no longer unchallenged, meaning the terrorist agenda that has dominated political concerns for decades is being supplanted by nation-state rivalries. The intelligence world has clearly recognised this challenge, and as is adjusting its priorities accordingly, but within any response espionage must play a vital role. While vast amounts of information can be gathered through open sources, Russia and China

are highly secretive regimes whose invasive controls expand to national and online media. Indeed, the very fact that Russia operates 'troll factories' is indicative of its efforts to control the narrative. Consequently, anything gleamed openly must not be considered a reflection of the truth, meaning if intelligence is to be acquired it must be done through far more surreptitious methods. While secrets can be collected through technical intelligence, whether through imagery satellites, eavesdropping, or even hacking, these methods are more constrained where highly guarded information is concerned. Imagery satellites can only see outside the building, eavesdropping is vulnerable to encryption, and most classified systems are air-gapped from the Internet, meaning they are almost impossible to hack. This, plus the benefits of discerning intentions, places greater onus on the value of the classic spy. More to the point, as Russia and China strengthen their defences, the gap that an agent can fill is likely to widen, creating more demand for high level espionage.

These issues carry through into counterintelligence, where it's clear that any effective defence must have an espionage component. One area of concern is that despite vast spending on cybersecurity, such measures alone are unlikely to mitigate Russian and Chinese cyber threats. That problem is exacerbated as the West adopts its own offensive posture, with each cyber breach potentially incurring tit-for-tat exchanges. Similar issues pertain to the rising number of Russian and Chinese intelligence officers operating on Western soil, who cannot be easily deterred through defensive practices. Although mass diplomatic expulsions have become something of a twenty-first century norm, both Moscow and Beijing boast the resources to replace their losses. These issues further increase demand for intelligence collection, to expose parties, tactics, and intentions. But since intelligence agencies are naturally among the hardest of hard targets, it is logical that they will be guarded against technical measures,

meaning if foreign intelligence activities are to be obstructed, espionage will play a primary role.

Overall, this chapter has shown that espionage has an important and growing role in the future of relations with Russia and China. But that shift from the entrenched world of counterterrorism towards nation states will be difficult. Through several decades of focus on the Middle East, the bulk of intelligence officers are unlikely to exhibit the language skills or tradecraft expertise necessary for operating in hard target conditions. Moreover, efforts to recruit a new generation of culturally experienced operatives have been soured by cases including Glenn Duffie Shriver's, with concerns of foreign intelligence-controlled candidates denying Langley some of its most fitting applicants. As a consequence, it will take time to train both seasoned officers and fresh practitioners from the ground up. Nonetheless, for all of the reasons explored above, it is a process that cannot be delayed, as espionage is clearly a vital component of the new security landscape, therefore showing it is highly important for intelligence officers to gain an advantage over these hard target states.

Chapter 3
The new spectre of street surveillance

Introduction

Having established the imperative for espionage against Russia and China, the next stage is to examine the argument for operational innovation. Therefore, this chapter will show how the spectre of street surveillance in major cities such as Moscow and Beijing, is forcing intelligence agencies to rethink their modus operandi. The central premise of this chapter is that while street surveillance is often a defining feature of hard target states, it is evolving in two key respects. First, it is becoming more ambitious and more aggressive, in parallel with Russia and China's waning tolerance for foreign espionage. Second, aided by proliferating technologies and a seemingly limitless surplus of data, street surveillance is growing more efficient and more precise. These factors, which place severe dangers over each interpersonal meeting, threaten espionage's effectiveness on an unprecedented level.

This chapter begins by examining the scope and scale of street surveillance in Russia and China. It shows how surveillance in both states is growing in manpower and aggression commensurate with their respective security concerns. Both states are fearful of spies within their ranks and are expanding their vast surveillance resources to keep foreign intelligence officers at bay. This problem is shown to be worsened through the proliferation and continued evolution of emerging surveillance developments. The first of these to be examined is biometrics, a border-crossing problem that threatens to expose undercover operatives from the moment they hand over their passport. In addition, the widespread availability of life history data, whether through stolen databases or easily accessible online sources, makes travel into foreign environments increasingly precarious. These, and other emerging issues, are shown to enhance the

threat of street surveillance, allowing counterintelligence to identify and observe foreign operatives with unprecedented efficiency.

The chapter concludes by examining the intelligence community's response. It argues that there are no simple solutions on the horizon, meaning intelligence officers must adapt to a new and unavoidable operational environment, where every meeting with a source has evolved into a point of extreme risk. Technological threats are already being adopted by Russian and Chinese security services, and in the current security climate it must be expected that street surveillance will only become more, not less, prominent an issue. Herein, a case for operational innovation, specifically cyber-enabled tradecraft, is presented through the reflections of the intelligence world's most senior figures, including the heads of SIS and CIA. Simply put, it shows how cyberspace is viewed as the potential solution to the surveillance problem.

Street surveillance in Moscow and Beijing

Regardless of the tradecraft at their disposal, most intelligence officers will, at some point, need to meet their agents face to face, but in doing so they must compete with espionage's Achilles Heel, *street surveillance*.[1] Practitioners regard surveillance as a pivotal defence against spying, 'the job of following and observing designated persons without being noticed, is intrinsic to counterintelligence' writes former CIA counterintelligence officer William Johnson, 'CI has so many uses for surveillance that I recommend no CI officer be promoted into management who has not himself been a

[1] Gioe, D. V. 'The more things change': HUMINT in the cyber age', in *The Palgrave Handbook of Security, Risk and Intelligence*, edited by Robert Dover, Huw Dylan, and Michael Goodman (London, Palgrave, Macmillan, 2017), p. 221-222.

surveillant on the streets….'[2] These sentiments are echoed by the CIA's former counterintelligence chief, James Olson:

> This is so fundamental to CI … Any CI program worthy of the name has to be able to engage the opposition on the street, the field of play for espionage. And when we do go to the street, we have to be the best service there. If we are beaten on the street, it is worse than not having been there at all … Opposition intelligence officers have to be watched, known meeting areas have to be observed, and, when an operation goes down — often on short notice — undetectable surveillance has to cover it, identify the participants, and obtain evidence.[3]

Owing to these risks, intelligence officers are trained to run *countersurveillance,* a form of tradecraft 'devoted primarily to frustrating this sort of activity'.[4] In addition to evasive manoeuvres, operatives will postpone meetings if surveillance teams are observed to preserve the identities of their contacts. To catch intelligence officers in the act, therefore, surveillance must remain hidden whilst covering enough ground to monitor the target throughout their journey, 'this is difficult and requires a great deal of manpower, since an officer trained in countersurveillance techniques will notice if the same person is trailing him for any length of time'.[5] Consequently, surveillance is often extremely expensive and requires vast resources. Liberal democracies have, in turn, often shied away from recruiting armies of surveillants, while authoritarian regimes have embraced it with open arms - indeed the defining feature of a "denied area" is the near inescapable scale of the state's surveillance.[6]

---

[2] Johnson, W. R. *Thwarting enemies at home and abroad: how to be a counterintelligence officer* (Washington, Georgetown University Press, 2009), p. 66.
[3] Olson, J. M. (14 April 2007) 'A never-ending necessity: the ten commandments of counterintelligence', *CIA.* Available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/fall_winter_2001/article08.html [accessed 17 July 2016].
[4] Shulsky, A. N. & Schmitt, G. J. *Silent warfare: understanding the world of intelligence,* (Washington, Brassey's, 2002), p. 109.
[5] Ibid.
[6] Redmond, P. 'The challenges of counterintelligence', in *Intelligence: The Secret World of Spies, an Anthology*, edited by Loch K. Johnson and James J. Wirtz (Oxford, Oxford University Press, 2011), p. 306.

The Russian government's willingness to invest vast resources in surveillance has become increasingly apparent. In the Cold War, closed borders ensured that only a handful of intelligence officers could travel into Moscow, most of whom were based in embassies under diplomatic cover and subjected to round-the-clock surveillance.[7] But the collapse of the Soviet Union offered only a temporary respite, as internal chaos, burgeoning organised crime, growing numbers of foreign intelligence officers, war in Chechnya, and low wages, stretched Russia's new security agency, the FSB (Federal'naia sluzhba bezopasnosti) to the brink.[8] However, with the aid of president Vladimir Putin, who regards the FSB 'as among his closest allies and most powerful instruments', the security service's powers have steadily increased.[9] Yet whereas the worst impulses of the KGB were reined in by party control, its successor is a far more autonomous beast, as Soldatov and Borogan write:

> These changes must not be mistaken for a revival of the Soviet KGB, although many former dissidents, journalists, and even the security services themselves have characterized it as such. The Soviet KGB was all-powerful, but it was also under the control of the political structure: The Communist Party presided over every KGB section, department, and division. It was no coincidence that the KGB was officially described as an "advanced regiment" of the party.
>
> In contrast, the FSB is a remarkably independent entity, free of party control and parliamentary oversight. If the FSB has an ideology, it is the goal of stability and order. FSB officers now regard themselves as heirs not only to the KGB but also to the secret police that the Tsars deployed to battle political terrorism.[10]

Since his tenure in the late 1990s as director of the FSB, Putin has increasingly called for greater need to tackle foreign espionage.[11] Declining relations with the West have

---

[7] Mendez, A. J. & McConnell, M. *The master of disguise: my secret life in the CIA*, [Kindle version] (New York, Harper Collins, 2007). Accessed 1 January 2018, p. 221-226.
[8] Brope, R. 'Russia', in *Routledge Companion to Intelligence Studies*, edited by Robert Dover, Michael S. Goodman, and Claudia Hillebrand, (Abingdon, Routledge, 2013), p. 231-234.
[9] Galeotti, M. (12 May 2017) Russian intelligence is at war, *NATO Review*. Available at: http://www.nato.int/docu/review/2017/Also-in-2017/russian-intelligence-political-war-security/EN/index.htm [accessed 24 October 2017].
[10] Soldatov, A & Borogan, I. *The new nobility: The restoration of Russia's security state and the enduring legacy of the KGB*, (New York, Public affairs, 2010), p. 4.
[11] Ibid, p. 35-36.

seen these fears escalate, with foreign spying rising to the state's top security priority.[12] In 2017, Putin declared that Russia faces 'greater demands' from foreign threats, particularly with regard to 'confidential information concerning our military-technical capability', and boasted about putting 'a stop to the work of 52 foreign intelligence officers and 286 agents' in the previous year.[13] To an extent, this rhetoric can be tied to rising political and social activism, since by labelling protestors as "paid agents of the West", Putin 'has the justification he needs to enact strict domestic security policies aimed at preventing the subversion of his administration and to eliminate his opponents.'[14] By accusing any serious opposition of being a puppet funded and controlled by Western intelligence agencies, Putin has essentially delegitimised political threats to his own regime.[15] But regardless of whether these claims are really believed by the Kremlin, the threat of foreign espionage and the surveillance of foreign operatives is increasingly central to Russian security, with Putin constantly bolstering his security services.[16] As of 2013, FSB's manpower was thought to number somewhere between 200,000 to 300,000, but this rose to 387,000 by 2016, which starkly compares to the SVR's meagre 13,000.[17]

[12] Parliamentlive.tv (8 March 2016) Russia: Implication for UK defence and security. Available at: http://parliamentlive.tv/Event/Index/f221826a-b5dd-4200-b00b-1bdf9d7a7c0e [accessed 10 January 2018].
[13] Official Internet Resources of the President of Russia (16 February 2017) Meeting of Federal Security Service Board. Available at: http://en.kremlin.ru/events/president/news/53883 [accessed 24 October 2017].
[14] Bateman, A., 'The political influence of the Russian security services', *The journal of Slavic military studies*, 27:3, 2014, p. 400.
[15] Ibid.
[16] Miller, G. (14 September 2016) As Russia reasserts itself, U.S. intelligence agencies focus anew on the Kremlin, *The Washington Post.* Available at: https://www.washingtonpost.com/world/national-security/as-russia-reasserts-itself-us-intelligence-agencies-focus-anew-on-the-kremlin/2016/09/14/cc212c62-78f0-11e6-ac8e-cf8e0dd91dc7_story.html?postshare=371473956824384&tid=ss_tw-bottom&utm_term=.d8941ad4f02e#comments [accessed 31 November 2017].
[17] Parliament (25 March 2016) Supplementary written evidence submitted by Dr Victor Madeira. Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/russia-implications-for-uk-defence-and-security/written/31103.pdf [accessed 2 January 2018], p. 1-3; Lucas, E. *Deception: Spies, lies, and how Russia dupes the West*, (London, Bloomsbury Publishing PLC, 2013), p. 68.

Given these numbers, anyone suspected of being an intelligence officer in Russia must expect near unrelenting scrutiny. According to former CIA officer Steve Hall, who served as Moscow Station's chief (*stations* are the CIA's regional espionage headquarters, which are usually based in US embassies), "[the] Russians make it extremely difficult for American intelligence officers to operate in Russia, in a way that would be nearly impossible for the F.B.I. to do the same".[18] Similar comments are echoed by Michael McFaul, who served as the US ambassador to Russia until 2014, "[the] counterintelligence operation that [Moscow] runs against the U.S. Embassy measures in the thousands … It always felt, especially sitting in Moscow, of course, that we were in a counterintelligence and collection battle that was an asymmetric fight."[19] The scale of this surveillance is matched by its intensity, with intelligence officers experiencing increasing levels of aggression by FSB watchers.[20] According to the *Washington Post,* McFaul was 'hounded by government-paid protesters, and intelligence personnel followed his children to school', while in Obama's first term 'Russian intelligence personnel broke into the house of the U.S. defense attaché and killed his dog'.[21] But these unpleasant incidents were only the beginning of a trend that worsened after Western sanctions in response to Russia's incursions in Ukraine.[22] As

[18] Schmidle, N. (7 August 2017) The U.S. has more to lose than Russia in spy expulsions, *The New Yorker.* Available at: https://www.newyorker.com/news/news-desk/the-us-has-more-to-lose-than-russia-in-spy-expulsions [accessed 10 January 2018].
[19] Miller, G. (14 September 2016) As Russia reasserts itself, U.S. intelligence agencies focus anew on the Kremlin, *The Washington Post.* Available at: https://www.washingtonpost.com/world/national-security/as-russia-reasserts-itself-us-intelligence-agencies-focus-anew-on-the-kremlin/2016/09/14/cc212c62-78f0-11e6-ac8e-cf8e0dd91dc7_story.html?postshare=371473956824384&tid=ss_tw-bottom&utm_term=.d8941ad4f02e#comments [accessed 31 November 2017].
[20] Schindler, J. R. (30 June 2016) Moscow rules of espionage go global – if you think it's KGB, it is: As Russian spies play rough, ignoring Putin's war against the West will only make it nastier, *Observer.* Available at: http://observer.com/2016/06/moscow-rules-of-espionage-go-global-if-you-think-its-kgb-it-is/ [accessed 11 January 2018].
[21] Rogin, J. (26 June 2016) Russia is harassing U.S. diplomats all over Europe, *The Washington Post.* Available at: https://www.washingtonpost.com/opinions/global-opinions/russia-is-harassing-us-diplomats-all-over-europe/2016/06/26/968d1a5a-3bdf-11e6-84e8-1580c7db5275_story.html?utm_term=.dab28978faf0 [accessed 11 January 2018].
[22] Ibid.

detailed in a report by Estonia's Teabeamet intelligence agency (and worth repeating in full), the tactics used by Russian security services against foreign officials appear to be increasingly dangerous, reckless, and audacious:

> • Traffic police stop vehicles with diplomatic plates with tiresome consistency and without reason. The tyres of diplomats' cars are punctured in parking areas;
>
> • Diplomats become embroiled in trouble with the police in order to be discredited. Fights are instigated, and accusations of shoplifting or pickpocketing levelled. Often organisers involve the media in such actions. These methods are effective against people where state secret clearance plays an important part in their activities, and whose reputations must, therefore, be spotless;
>
> • Diplomats are attacked and beaten up by "unknown individuals" or their drinks are spiked with intoxicating substances in public entertainment venues, without anything being stolen from the victim. Investigations by the Russian authorities usually lead nowhere and the culprits are never found;
>
> • The FSB covertly directs and controls the activities of a large share of Russian media outlets. The FSB tips off its media contacts as to the diplomats' plans; a meeting of a diplomat and local opposition activist in some cafe may be interrupted by a TV station crew, which starts grilling both of them in front of the cameras about the purpose of their meeting;
>
> • Interviews conducted in such a manner or e-mails, photos and screenshots of social media posts recorded secretly by the FSB (some of them falsified as well) and "leaked" onto the Internet have on many occasions been used during prime time programming on major state-controlled TV stations as a part of "documentary films" and talk shows. On these programmes, the non-systemic opposition is accused of plotting to overthrow the "democratic" state order in Russia, and Western diplomats – whom the producers allege are colluding with the intelligence services of their respective countries – are charged with recruiting, handling and funding Russians. Usually, such scenarios are supported by interviews with Russian "experts", who cite the same kinds of chaos, said to be fomented [sic] by the West, in the Middle East and North Africa, Ukraine and Georgia. In general, Russian television claims that the local opposition is preparing a "colour revolution" with the connivance of foreign countries;
>
> • Breaking into diplomats' apartments and leaving "calling cards" – meaning identifiable traces. Nothing is taken from the apartments – the purpose is to show the resident that it was not a burglary. The media describes such FSB "calling cards" left in these apartments as rearranged furniture, home appliances and lights left on, and excrement on the carpet. In one case, a dog in a diplomat's apartment was killed. The imagination of the harassers knows no bounds when it comes to "redecorating" the diplomats' apartments. As in the case of physical assaults on diplomats, the intruders are never found.

> • Russian authorities usually deny consistent, coordinated harassment of foreign diplomats. If the events do become public, the Russian Foreign Ministry mainly uses one of two tactics: either it mocks the accusations from the West ("sick fantasy" or "dime store detective novel") or it resorts to whataboutism, a time-honoured propaganda tactic. The ministry will accuse [the] Western countries themselves of violating the rights of Russian citizens. These, however, do not involve harassment of Russian diplomats; rather, the ministry cites arrests of criminals who are Russian citizens or the alleged abuse of children adopted from Russia.[23]

In some cases, this has forced intelligence officers to evacuate Moscow, as exemplified in 2016 when one US diplomat (confirmed to be a CIA officer) was violently tackled to the ground by a uniformed FSB guard as he returned to the embassy.[24] The attack was allegedly provoked when the CIA officer successfully lost his tail, infuriating the FSB who responded with injuries severe enough to merit an immediate medical flight out of Moscow.[25] Previously, aggressive harassment of this nature was mostly reserved for intelligence officers who provoked their watchers, but evidently this unwritten rule of espionage is being ignored.[26] In 2016, these tactics led the then serving director of the CIA, John Brennan, to raise the issue with his FSB counterpart, Alexander Bortnikov, 'I first told Mr Bortnikov, as I had several times previously that the continued mistreatment and harassment U.S. diplomats in Moscow was irresponsible, reckless, intolerable and needed to stop'.[27] Despite this effort, within a year US diplomats and

[23] Teabeamet Estonian Information Board (2017) 'International security and Estonia'. Available at: https://www.valisluureamet.ee/pdf/2017-en-c482143c.pdf [accessed 24 October 2017], p. 26.
[24] Watkins, A. (1 June 2017) Russia escalates spy games after years of US neglect, *Politico*. Available at: https://www.politico.eu/article/russia-escalates-spy-games-after-years-of-us-neglect/ [accessed 24 October 2017].
[25] Ibid.
[26] Schindler, J. R. (30 June 2016) Moscow rules of espionage go global – if you think it's KGB, it is: As Russian spies play rough, ignoring Putin's war against the West will only make it nastier, *Observer*. Available at: http://observer.com/2016/06/moscow-rules-of-espionage-go-global-if-you-think-its-kgb-it-is/ [accessed 11 January 2018].
[27] CNN (23 May 2017) Transcripts. Available at: http://transcripts.cnn.com/TRANSCRIPTS/1705/23/cnr.03.html [accessed 24 October 2017].

their families were constantly reporting acts of intimidation and harassment by Russian security services throughout Moscow and Europe.[28]

Moreover, any hope of trying to meet sources and agents in less hostile environments has been curtailed by travel restrictions. As argued by *The Moscow Times* (one of few Russian media outlets not controlled by the state), '[an] important part of the Kremlin's new course of self-imposed isolation is the rapid growth in the number of citizens who, for various reasons, are banned from leaving the country', particularly those employees 'in the country's bloated security apparatus'.[29] The FSB's staff were one of the first to be restricted after one officer, Aleksandry Poteyev, defected to the US in 2010, revealing the names of the Russian Illegals arrested that same year. Since the Ukraine conflict the outreach of travel bans has vastly expanded, including over 4 million Russian personnel in government, military, and security sectors. The Ministry of Defence alone accounts for two million employees who now cannot travel to a list of around 150 countries without permission. This list also extends to top-ranking officials, 'Defense Minister Sergei Shoigu, Federal Drug Control Service chief Viktor Ivanov, Federal Security Service head Alexander Bortnikov and others are, like the lower-ranking members of their agencies, affected by the ban and cannot visit the West'.[30] Simply put, if intelligence offers are to meet with sources who can access classified information, they will more than likely have to do so in Moscow, where FSB surveillance is at its most effective, aggressive, and resourced.

[28] Rogin, J. (26 June 2016) Russia is harassing U.S. diplomats all over Europe, *The Washington Post.* Available at: https://www.washingtonpost.com/opinions/global-opinions/russia-is-harassing-us-diplomats-all-over-europe/2016/06/26/968d1a5a-3bdf-11e6-84e8-1580c7db5275_story.html?utm_term=.dab28978faf0 [accessed 11 January 2018].
[29] Ryzhkov, V. (16 May 2014) Controlling Russians through travel bans, *The Moscow Times.* Available at: https://themoscowtimes.com/articles/controlling-russians-through-travel-bans-35830 [accessed 11 January 2018].
[30] Ibid.

The state of affairs in China has drawn considerably less media attention, but it's clear that Beijing puts surveillance at the forefront of its security. Traditionally, counterintelligence fell under the Ministry of Public Security (MPS), but following the economic reforms of Den Xiaoping in 1979, many of the MPS's powers were absorbed by the Ministry of State Security (MSS), established in 1983.[31] With the separation, MSS not only took the lead in foreign intelligence gathering (which it also absorbed from the Investigation Department), it also took control of counterintelligence missions including street surveillance and technical eavesdropping.[32] The MPS is still responsible for policing and public order, but the MSS absorbed all offensive and defensive aspects of intelligence under one house.[33] In recent years, owing in part to China's large and growing international community, the budgets of MPS and MSS have grown considerably.[34] By 2010 alone, China's internal security budget outstripped its immense military modernization budget by several billion, rising to $111 billion in 2012.[35] While the portion of that funding spent on counterintelligence remains unclear, it emphasises China's voracious appetite for security.

But that appetite is still growing, as the threat of foreign espionage continues to alarm Chinese policymakers. Even by the end of the Cold War, concerns of foreign espionage were high on the agenda. According to one leaked MSS document from the 1990's, China perceived foreign diplomats as "open spies", and placed numerous

[31] Guo, X. *China's security state: philosophy, evolution, and politics*, (New York, Cambridge University press, 2012), p 437.
[32] Inkster, N. 'Chinese intelligence in the cyber age', *Global politics and strategy*, 55:1, 2013, p. 48; Stratfor (March 2010) Intelligence services, part 1: Espionage with Chinese characteristics, *WikiLeaks*. Available at: https://WikiLeaks.org/gifiles/attach/133/133464_INTEL_SERVICES_CHINA.pdf [accessed 11 January 2018].
[33] Ibid.
[34] Mattis, P. 'Beyond spy vs. spy: the analytic challenge of understanding Chinese intelligence services', *Studies in Intelligence*, CIA, 56:3, 2012, p. 50.
[35] Ibid.

international journalists and business travellers under surveillance.[36] By the 1990s, Chinese policymakers exhibited 'what might be described in Western terms as a paranoiac fear of foreign influence', but that fear has since worsened.[37] In 2011, Major General Jin Yinan, speaking at what he wrongly believed to be a private conference, discussed several cases in which officials were found to be spying for foreign powers.[38] One such case included Kang Rixin, a member of the CCP's Central Committee, and head of China's National Nuclear Corporation. Kang was publicly jailed for bribe-taking, but in fact, he was imprisoned for life after spying for an undisclosed foreign intelligence agency. Knowing that spies such as Kang were active in the CCP's highest ranks made policymakers "extremely nervous", but those fears were put on a legal footing in 2014, when Beijing replaced its 1993 National Security Law with a new Counterespionage Law, which grants greater powers for acting against foreign intelligence officers and 'Chinese collaborators'.[39]

As analyst Scot Tanner told *The New York Times*, the law "inevitably sends a message that the party is concerned about – and may intend to more closely monitor – the relationships between many of its citizens and the international community with which China is increasingly intertwined."[40] Since this point, street surveillance against intelligence officers and diplomats in Beijing has grown in intensity and aggression.[41]

---

[36] Stratfor (March 2010) Intelligence services, part 1: Espionage with Chinese characteristics, *WikiLeaks*. Available at: https://WikiLeaks.org/gifiles/attach/133/133464_INTEL_SERVICES_CHINA.pdf [accessed 11 January 2018], p. 4-9.
[37] Eftimiades, N. *Chinese Intelligence Operations*, [Kindle version] (Ilford, Frank Cass, 1994). Accessed 10 January 2018, chapter six.
[38] Brookes, A. (4 November 2014) Is China swarming with foreign spies?, *Foreign Policy.* Available at: http://foreignpolicy.com/2014/11/04/is-china-swarming-with-foreign-spies/ [accessed 11 January 2018].
[39] Ibid.
[40] Tatlow, D. K. (2 November 2014) China approves security law emphasizing counterespionage, *The New York Times.* Available at: https://www.nytimes.com/2014/11/03/world/asia/china-approves-security-law-emphasizing-counterespionage.html?ref=asia [accessed 11 January 2018].
[41] Watkins, A. (10 November 2017) China grabbed American as spy wars flare, *Politico.* Available at: https://www.politico.com/story/2017/10/11/china-spy-games-espionage-243644 [accessed 11 January 2018].

As one American official noted, Chinese surveillance teams "were as fundamentally aggressive in their activity [as the Russians] … They always knew what we were doing and where we were."[42] Although the official described Chinese surveillance as more "subtle" than their Russian counterparts, some incidents show a more dangerous trend.[43] US officials told *Newsweek* that entrapment, through the rampant deployment of prostitutes, is a common tool of Chinese security services, which became a critical issue during the 2008 construction of the US embassy in Beijing, "[we] were constantly having to send people home for fraternization … That was a very big problem, keeping construction crews on site, because the Chinese clearly were trying to target them, but we kept a pretty careful handle on all of that".[44] More recently, US diplomats in China have reported constant and intense surveillance, alongside more intimidating tactics such as their apartments being broken into and "tossed" (overtly searched).[45] But in 2016, an official from the US consulate in Chengdu was kidnapped, interrogated, and forced to confess to acts of treachery by plainclothes security officers. The American, who was suspected of being a CIA officer, was eventually released and evacuated from the country, but the case is considered an 'extreme illustration' of the state of surveillance in Beijing.[46]

Akin to Russia, travel restrictions ensure that if intelligence officers want to meet high valued Chinese sources, they're more than likely going to have to do so in these hostile conditions, as *Foreign Policy* reports:

> According to interviews with several people close to the ruling party leadership, ex-Politburo members are not allowed to travel overseas without permission

[42] Ibid.
[43] Ibid.
[44] Stein, J. (22 May 2017) Chinese counterspies roiling U.S. intelligence operations in Beijing, *Newsweek*. Available at: http://www.newsweek.com/chinese-counterspies-roiling-us-intelligence-operations-613393 [accessed 11 January 2018].
[45] Watkins, A. (10 November 2017) China grabbed American as spy wars flare, *Politico*. Available at: https://www.politico.com/story/2017/10/11/china-spy-games-espionage-243644 [accessed 11 January 2018].
[46] Ibid.

> from the current PBSC. "It's the accepted custom," said someone with ties to the leadership, who asked to remain anonymous because of the sensitivity of the issue. This rule applies to dozens of members of China's political elite, including both living ex-presidents: Jiang Zemin, rumored to be under suspicion for corruption, and Hu Jintao, who is untainted by allegations of graft, said someone with ties to the leadership.[47]

According to one anonymous expert on Chinese leadership, the rule is so tight that few, if any, former leaders are allowed to travel abroad - as China specialist David Lampton adds "[in] China, ex-leaders basically don't leave the country".[48] Moreover, outside of work-related circumstances, serving Politburo members cannot travel abroad for more than one trip a year, and even then, only for a handful of days. As further argued by specialist on Chinese leadership, Bo Zhiyue, "[these] people have a lot of secrets … if there is a way to block that person [from leaving], they will do so."[49] As a consequence, like their colleagues in Moscow Station, intelligence officers will need to pursue most of their quarry in Beijing, where they are far more vulnerable to the MSS's increasingly intensive and aggressive surveillance resources.

The problem of 'cover' in the digital age

Even with vast resources, the manpower required to keep one person under observation makes it important to target surveillance at actual intelligence officers.[50] However, in order to frustrate surveillance, intelligence officers rely on cover, which is essentially a fake identity designed to blend operatives into foreign environments.[51] Most operatives rely on *official cover,* posing as diplomats within their government's respective embassies. In this role, officers can interact with foreign officials, and benefit from the

[47] Fish, I. S. (24 December 2015) Why can't ex-Chinese leaders travel abroad, *Foreign Policy.* Available at: https://foreignpolicy.com/2015/12/24/why-are-former-chinese-leaders-prevented-from-traveling-overseas-xi-jinping/ [accessed 11 January 2018].
[48] Ibid.
[49] Ibid.
[50] Shulsky, A. N. & Schmitt, G. J. *Silent warfare*, p. 109.
[51] Ibid, p. 12

protections of diplomatic immunity.[52] Official cover operatives are, however, usually easier to spot, simply by observing embassy patterns of activity.[53] The alternative is *nonofficial cover,* such as travelling under business aliases, that provides access to sources who are not on the diplomatic circuit.[54] The downside to nonofficial cover is that maintaining the illusion of a businessman may require the intelligence officer to work a full-time job, either by establishing their own business or finding a cooperative front company.[55] Whichever option the intelligence officer adopts, the defensibility of cover is seen to be increasingly under threat, owing to a confluence of emerging and proliferating technologies.[56] As Lord argues:

> … today's emerging digital environment has the potential to wholly transform the foundation upon which intelligence rests: secrecy … In a digital world those cover identities and tradecraft manufactured for an analog environment can quickly become ineffective and potentially dangerous to those who continue to use them.[57]

Many of these issues emerge during the crossing of borders, an event that is becoming 'particularly hazardous for the international traveller'.[58] One key problem is biometrics, which are 'the cornerstone of a physical identification', drawn from features that 'cannot be changed without either a medical procedure or injury, down to the DNA, with very few exceptions.'[59] Biometrics are used by governments around the world for a multitude of purposes, including 'when issuing licenses, identifying corpses, prosecuting criminals, and as security measures to access protected areas or computer

[52] Ibid.
[53] Ibid, p. 109.
[54] Ibid, p. 13.
[55] Ibid.
[56] Lord, J. 'Undercover under threat: Cover identity, clandestine activity, and covert action in the digital age', *International Journal of Intelligence and Counterintelligence,* 28:4, 2015, p. 666.
[57] Ibid.
[58] Clark, R. *Intelligence collection,* (Thousand Oaks, CQ Press, 2014), p. 60-61.
[59] Shavers, B. & Bair, J. *Hiding behind the keyboard: uncovering covert communication method with forensic analysis,* [Kindle version] (Cambridge MA, Syngress, 2016). Accessed 10 January 2018, p. 187-188.

systems.'[60] They are also increasingly prevalent in border crossings and airports.[61] By 2010, for example, EU member states began building a joint 'Visa Information System', to 'store for five years fingerprints and photographs from 20m applicants each year for visas to enter the Schengen area', which 'will be available for immigration purposes but also available for the investigation of serious criminal offences.'[62] Similarly, '[the] US takes photographs and all ten fingerprints from each arriving visitor under its US-VISIT programme.'[63] China is trialling biometric systems in Shenzhen Bao'an international Airport, to fingerprint all foreigners aged between 14-70 entering the country.[64] In 2014 Russia adopted Executive Order 735, requiring collection of biometric data (fingerprints) of 'all foreign nationals and stateless persons for each of their application for Russian visa.'[65] The Ministry of Foreign Affairs was sure to insist that its actions followed global norms:

> The fingerprinting procedure should not be considered as a tightening of Russia's visa policy, but rather an essential element of its modernization. The use of additional biometrics in visa procedures for Russian citizens has been practiced for several years by the consular services of the US and the UK. The European Union countries are planning to introduce this procedure for Russian citizens in April 2015. The main objective of the new procedure is to improve the security of the visas issued in the context of preventing illegal migration, terrorism and other illegal activities.[66]

The problem is that if an intelligence officer passes through a biometric system for the first time, whichever identity they adopted will be permanently tied to their own

[60] Ibid.
[61] Stein, J. (4 December 2012) CIA's secret fear: high-tech border checks will blow spies' cover, *Wired*. Available at: https://www.wired.com/2012/04/cia-spies-biometric-tech/ [accessed 11 January 2018].
[62] Brown, I. 'Data protection: The new technical and political environment', *Computers & Law*, 20:6, 2010, p. 2-3.
[63] Ibid.
[64] Independent (9 February 2017) China to take fingerprints of all foreign travellers entering country. Available at http://www.independent.co.uk/news/world/asia/china-fingerprints-tourist-visits-scanning-customs-a7571871.html [accessed 11 January 2017].
[65] The Ministry of Foreign Affairs of Russia (3 December 2014) About the new requirement for foreign nationals and stateless persons to provide their biometric data when applying for Russian visas on the territory of the United Kingdom. Available at: https://www.rusemb.org.uk/consnews/29 [accessed 11 January 2018].
[66] Ibid.

biometrics. "[It's]s a one-time thing – one and done", argued one former CIA officer, "[the] biometric data on your passport, and maybe your iris, too, has been linked forever to whatever name was on your passport the first time."[67] Therefore, whereas previously, undercover travellers relied on forged passports and papers, which were laboriously difficult to differentiate from legitimate paperwork, today's cover identities can be unravelled with a single biometric scan.[68]

In keeping with international norms, Russia does not collect biometrics 'when issuing diplomatic and official visas', nor does China.[69] However, any diplomats pulled aside for airport 'secondary screening', a process of additional scrutiny by security officers for select travellers, may have their biometrics tested.[70] As described by leaked CIA documents from Wikileaks, 'resulting secondary screening can involve in-depth and lengthy questioning, intrusive searches of personal belongings, cross-checks against external databases, and collection of biometrics – all of which focus significant scrutiny on an operational traveler.'[71] Undercover travellers can be pulled for screening if they appear on watchlists of suspected intelligence officers, but other causes include random selection, errors or inconsistencies in travel documentation, suspicious behaviour, nationality, travel pattern, person-of-interest watchlists, or even as an attempt to elicit bribes by airport officials.[72] Simply put, there are multiple reasons why

[67] Stein, J. (4 December 2012) CIA's secret fear: high-tech border checks will blow spies' cover, *Wired.* Available at: https://www.wired.com/2012/04/cia-spies-biometric-tech/ [accessed 11 January 2018].
[68] Ibid.
[69] The Ministry of Foreign Affairs of Russia (3 December 2014) About the new requirement for foreign nationals and stateless persons to provide their biometric data when applying for Russian visas on the territory of the United Kingdom. Available at: https://www.rusemb.org.uk/consnews/29 [accessed 11 January 2018]; Zhou, M. (2 November 2017) Fingerprinting of foreign visitors gets started at Shenzhen's Bao'an Airport, *China Daily*. Available at: http://www.chinadaily.com.cn/china/2017-02/11/content_28168119.htm [accessed 11 January 2018].
[70] CIA (21 December 2014) CIA assessment on surviving secondary screening at airports while maintaining cover, *WikiLeaks.* Available at: https://WikiLeaks.org/cia-travel/secondary-screening/WikiLeaks_CIA_Assessment_on_Surviving_Secondary_Screening.pdf [accessed 11 January 2018], p. 3.
[71] Ibid.
[72] Ibid, p. 6-11.

an operative might be led to secondary screening - one CIA officer was even screened, they suspect, for wearing 'overly casual dress inconsistent with being a diplomatic-passport holder.'[73] Either way, it underscores the point that no form of cover is immune to the biometric problem.

One intelligence officer suggests avoiding biometric borders altogether: "[as] a hypothetical, why fly into Frankfurt if it has all the newest biometric gear when you can fly into Split, Croatia, or Ljubljana, Slovenia, and drive to Frankfurt?"[74] But in addition to the proliferation of biometrics in border crossings, hotels and car rentals are also likely to conduct passport checks, as Stein explains:

> Even crossing the border with a real identity, then donning a fake one in-country, presents its own risks. "When you go to check into a hotel room for a meeting with an asset, or even rent a car to drive to the meeting — or hold the meeting *in* the car — many hotels and car rental agencies upload their customer data, including passport number, to immigration every day," the former spook notes. "Most countries are looking for visa overstays. But when you show up on the list as never having entered the country … it brings the police around to ask questions."
>
> Often, a CIA operations officer travelling under nonofficial cover … can pick up a new set of documents from a CIA courier or dead drop since he or she is in the country. There's nothing new about that. But since the better hotels require guests to present their passports, which are scanned into the system, the ruse is increasingly rendered moot, especially in hostiles climes like Iran, where the interior ministry's computer are assumed to be hard-wired into the airline passenger and hotel guest lists.
>
> One obvious workaround is for operatives to book one-star hotels where such impediments are less likely. But if they're traveling undercover as, say, a prosperous Western business executive, booking a room in a seedy joint only raises red flags with the desk clerks and local gendarmes.[75]

However, biometric scans are not entirely flawless, '[each] biometric comes with strengths and weaknesses, and with a full knowledge of these pros and cons the system

[73] Ibid, p. 14.
[74] NewsRep (24 March 2015) How technology is changing the future of espionage. Available at: https://thenewsrep.com/40315/technology-changing-future-espionage/#ixzz3imhEq0HG [accessed 23 February 2018].
[75] Stein, J. (4 December 2012) CIA's secret fear: high-tech border checks will blow spies' cover, *Wired.* Available at: https://www.wired.com/2012/04/cia-spies-biometric-tech/ [accessed 11 January 2018].

can be cheated.'[76] Fingerprints offer around 98-100 percent accuracy, but deteriorate over time due to cuts and scars, while iris scans are almost infallible yet also time consuming.[77] The margin for error is small, but when applied across millions of yearly travellers the chances of encountering a false-positive substantially increase, as Enerstvedt adds, 'the more biometric identification is used and the larger the database, the greater the likelihood of false matches'.[78] Furthermore, it must be noted that most airports test biometrics for law enforcement purposes, meaning biometric alerts among certain travellers may draw less scrutiny.[79] As a second CIA document released by Wikileaks notes, the 'European Union's Schengen biometric-based border-management systems pose a minimal threat to US operational travelers because their primary focus is illegal immigration and criminal activities, not counterintelligence, and US travelers typically do not fit the target profiles'.[80] By comparison, a CIA operative who fails a biometric test in a Moscow airport should expect a far less cordial response, and will almost certainly be pulled aside for secondary screening.[81]

If pulled into secondary screening, intelligence officers, particularly non-official cover travellers, face further challenges. At the surface level, a person's social media history can be quickly checked by any security officer armed with a laptop, meaning

[76] Streeter, D. C. 'Biometrics and intelligence asset protection: Biometric technology and its impact on counterintelligence and intelligence', *Liberty University Helm's School of Government,* 2013, p. 11.
[77] Ibid, p. 12-13.
[78] Enerstvedt, O. M., *Aviation security, privacy, data protection and other human rights: technologies and legal principles*, (Cham, Springer international publishing, 2017), p. 253.
[79] Streeter, D. C. 'Biometrics', p. 12-13.
[80] CIA (21 December 2012) CIA advice for US government operatives infiltrating Schengen, *WikiLeaks.* Available at: https://WikiLeaks.org/cia-travel/infiltrating-schengen/WikiLeaks_CIA_Advice_for_Operatives_Infiltrating_Schengen.pdf [accessed 11 January 2018], p. i.
[81] CIA (21 December 2014) CIA assessment on surviving secondary screening at airports while maintaining cover, *WikiLeaks.* Available at: https://WikiLeaks.org/cia-travel/secondary-screening/WikiLeaks_CIA_Assessment_on_Surviving_Secondary_Screening.pdf [accessed 11 January 2018], p. 13.

they would need a digital presence to match their alleged identity.[82] As the CIA's secondary screening document explains:

> Internet access also allows airport security officials to examine travelers' social and business network accounts to confirm that their Web presence corresponds with their persona. For example, Foursquare and Linked-In are business equivalents to the Facebook social network. Security officials might also expect a sales or marketing traveler to have a Twitter account. The absence of such business-related Web accounts probably would raise a business traveler's profile with officials.[83]

Herein lies a key dilemma - if intelligence officers provide these accounts, the first question any counterintelligence officer will ask is 'how far back does it go?'[84] The alleged high-flying businessman with only six months of social media presence would look immediately suspicious, but on the flipside, if operatives create fake profiles packed with information, they risk overcomplicating their cover. As Gioe notes, '[if] pressed, he could have to describe his office building, his parking garage, his favorite lunch place, or his daily commute in ways that could be easily checked in Google Earth or similar commercially available mapping software.'[85] The CIA's guidelines for this problem are supposedly 'thin', and stress that revealing 'too much on Facebook and Twitter risks tipping too much to the other side', while 'revealing too little could also arouse suspicion'.[86] Privacy settings offer some defence, but security officers could demand access to a person's accounts during secondary screening. Indeed certain visa

[82] Gioe, D. 'The more things change', p. 217-218.
[83] CIA (21 December 2014) CIA assessment on surviving secondary screening at airports while maintaining cover, *WikiLeaks.* Available at: https://WikiLeaks.org/cia-travel/secondary-screening/WikiLeaks_CIA_Assessment_on_Surviving_Secondary_Screening.pdf [accessed 11 January 2018], p. 12.
[84] Gioe, D. 'The more things change', p. 217-218.
[85] Ibid.
[86] Troianovski, A. (16 May 2013) Social media pose new riddle for CIA, *The Wall Street Journal.* Available at: https://www.wsj.com/articles/SB10001424127887323398204578487173173371526 [accessed 11 January 2018].

travellers to Russia and the US are required to surrender social media history in advanced (five years' worth in the US case).[87]

This is only the surface level of a far deeper 'digital exhaust' problem, much of which extends beyond the individual's control. For example, photographs posted by friends and family on social media can be tied to a traveller's alias through facial recognition software.[88] As Mahmood demonstrates, if an operative based in the Middle East builds a Facebook cover profile, Facebook's automated facial recognition software might identify his photos and send 'tagging' requests to his real life friends and family, drawing a link between his fabricated and real identities.[89] What's more, facial recognition capabilities continue to evolve, an issue that only worsens as more people continue to post more images on social media.[90] For instance, one highly popular tool is Russia's *FindFace,* which matches social media photos with around seventy percent reliability.[91] The tool's developers poignantly add that "if the FSB were to get in touch, of course we'd listen to any offers they had".[92]

Beyond social media, a greater concern is private data stored within large government and commercial databases, as former intelligence officer Nigel Inkster argues, "[wherever] we go in today's world we leave a digital footprint – a digital

---

[87] Huffington Post (3 June 2019) Nearly all U.S. visa applicants now required to submit 5-year social media history. Available at: https://www.huffingtonpost.co.uk/entry/visa-social-media-state-department_n_5cf4898ce4b0e8085e3bfde1?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAImALRHTwaQyk9Lu3BCqYlCdJjsHnXXur6Gu-UCvjyknbwpH-hjDYnM_5gsx3zelhVO05YVF_migMklpe3CyyQvPSHXaituIb3iLew56P8YH3_0i40dTZkT3LVrkSRhauyRuNwT_MGWfP4c8tkQaeWpPkDnKyAr0a1ANiCQdfIqo [accessed 10 July 2019].
[88] Mahmood, S. 'Online social networks and terrorism: threats and defenses', in S*ecurity and Privacy Preserving in Social Networks,* edited by Richard Chbeir & Bechara Al Bouna (London, Springer, 2013), p.85.
[89] Ibid.
[90] Norval, A. & Prasopoulou, E. 'Public faces? A critical exploration of the diffusion of face recognition technologies in online social networks', *New media & society,* 19:4, 2017, p. 638.
[91] Walker, S. (17 May 2016) Face recognition app taking Russia by storm may bring end to public anonymity, *The Guardian.* Available at: https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte [accessed 11 January 2018].
[92] Ibid.

exhaust."[93] This risk was emphasised in the fallout of the CIA's abduction of Abu Omar from the streets of Milan in 2003, where Italian security services used digital forensic methods to expose and convict twenty-three CIA officers for kidnapping.[94] Investigators identified the CIA operatives' SIM cards in the kidnapping zone, which they used as a starting point to trace their pattern of travel, '[an] analysis of these SIMs and their geo-locations on the day of the kidnapping led prosecutors to suspect a complex operation of multiple teams, some directly involved, some in support'.[95] The SIMs eventually led to the operatives' personal addresses, hotel check-ins, and credit cards, all pointing to their intelligence roles. For example, 'addresses left at hotels were almost all based in 'D.C.'s Virginia suburbs', while their credit cards 'shared as many as the first 14 to 16 digits, pointing to a common origin'.[96] The investigation's purpose was to prove CIA culpability in a criminal case, but the same information could be just as easily applied to counterintelligence:

> Had this investigation been conducted by an organization with a counterintelligence mission, the investigators would likely have simply continued to collect data and monitor the movement and activities of identifiable officers and artifacts (cellphones, etc.) while mapping other nodes within the broader CIA network. Mapping the identity of the CIA's officers and operations throughout Europe might then have become possible.[97]

Recent reports by Bellingcat show how powerful digital history can be for investigative sleuths. Not only did their researchers thoroughly expose the three GRU operatives who tried to assassinate Sergei Skripal in 2018, but by scouring databases and passport records they quickly traced their operations throughout Europe.[98] However,

---

[93] Jones, S. (28 September 2016) The spy who liked me: Britain's changing secret service. *Financial Times.* Available at: https://www.ft.com/content/b239dc22-855c-11e6-a29c-6e7d9515ad15 [accessed 1 March 2018].
[94] Lord, J. 'Undercover under threat', p. 669-671.
[95] Ibid.
[96] Ibid.
[97] Ibid.
[98] Bellingcat (20 September 2018) Skripal suspects confirmed as GRU operatives: prior European operations disclosed. Available at: https://www.bellingcat.com/news/uk-and-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-european-operations-disclosed/ [accessed 10 July 2019].

Bellingcat's exposé would not have been possible without the closed-circuit footage that initially tied the suspects to the scene. The operational hazards of CCTV were also underscored in 2010, when Dubai authorities collated camera footage with cell phone records to identify and track the Israeli Mossad team responsible for assassinating Mahmoud Al-Mabhouh.[99] As Inkster elaborates:

> The Dubai authorities' investigation, relying on CCTV footage, revealed that the assassination team consisted of at least 18 people, some of whom had entered hotel washrooms which they then exited having altered their appearance. All were travelling on false identities using UK, Republic of Ireland, Australian, French or German passports in identities which had been stolen from individuals, some of whom were residents of Israel.[100]

Disguises may have been an effective countermeasure against physical watchers, but they were not enough for Mossad to fool the thousands of images recorded in Dubai's luxury hotels.[101] This problem cannot be easily resolved in surveillance states - China reportedly operated around 170 million cameras in 2017 alone, a figure set to rise to 400 million by 2020.[102] It also claims to have achieved one-hundred percent coverage of Beijing, with networks of cameras dissected into specific grids for streamlined surveillance.[103] As China expert Ai Xiaoming notes, the system "has been developed with the aim of tightening control, including of people who are critical of the government", with each grid coordinating with security services, party officials, and government entities to keep key targets under watch.[104]

---

[99] Inkster, N. 'Intelligence agencies and the cyber world', *Strategic Survey*, (2012), p. 46.
[100] Ibid.
[101] BBC News (28 March 2010) Dubai's starring role in Israeli-linked murder plot. Available at: http://news.bbc.co.uk/1/hi/world/middle_east/8588873.stm [accessed 21 August 2020].
[102] BBC News (10 December 2017) In your face: China's all-seeing state. Available at: http://www.bbc.co.uk/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state [accessed 11 January 2018].
[103] Yin, C. (10 March 2015) More 'eyes' fight crime in crowds, *China Daily*. Available at: http://www.chinadaily.com.cn/china/2015-10/05/content_22091634.htm [accessed 11 January 2018]; Callick, R. (9 December 2016) China's all-seeing spy grid takes surveillance to new level, *The Australian.* Available at: http://www.theaustralian.com.au/news/inquirer/chinas-allseeing-spy-grid-takes-surveillance-to-new-level/news-story/7dfdf3fef86da6b8203c6acba3840539 [accessed 11 January 2018].
[104] Ibid.

China is also rolling out a more advanced network of CCTV combined with facial recognition software to identify targets automatically.[105] As disclosed in a 2017 *BBC News* report, the system is being trialled in the city of Guiyang, where all residents are digitally catalogued, with their images fed into a central police hub directly connected to the city's CCTV. This complex system includes the prolific application of cameras equipped with artificial intelligence software, which are able to match individual faces in a crowd, as well as 'estimate age, ethnicity and gender.'[106] As explained by one of the technology's architects, "[we] can match every face with an ID card and trace all your movements back one week in time. We can match your face with your car … match you with your relatives and the people you're in touch with. With enough cameras, we can know who you frequently meet."[107] The state takes this technology extremely seriously - Beijing is experimenting with multiple facial recognition networks of its own, while China's police are allegedly set to invest $30 billion in similar technologies on a national level.[108]

Similarly, by 2017 Moscow already boasted around 146,000 surveillance cameras.[109] But according to investigative researchers, Soldatov and Borogan, the authorities are trialling an advanced CCTV network of their own, using 'multibiometric systems for identifying individuals in real time'.[110] This technology means the camera

[105] BBC News (10 December 2017) In your face: China's all-seeing state. Available at: http://www.bbc.co.uk/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state [accessed 11 January 2018].
[106] Ibid.
[107] Ibid.
[108] Mozur, P. (8 July 2018) Inside China's Dystopian Dreams: A.I, shame and lots of cameras, *The New York Times.* Available at: https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html [accessed 24 October 2020].
[109] CNN (14 June 2017) 146,000 cameras monitor Moscow streets. And the government is just getting started. Available at: http://money.cnn.com/2017/06/14/technology/culture/moscow-cameras/index.html [accessed 11 January 2018].
[110] Soldatov, A. & Borogan, I. (15 November 2011) A face in the crowd: the FSB is watching you!, *open Democracy.* Available at: https://www.opendemocracy.net/od-russia/andrei-soldatov-irina-borogan/face-in-crowd-fsb-is-watching-you [accessed 11 January 2018].

can ‘pick out your face in a crowd, compare it with a database and determine whether you are a criminal, or even establish your identity.’[111] Moreover, the project is being carried out under the auspices of the FSB:

> For example, on 8 October 2009, when two projects were discussed – one the creation of an automated video system for detection and identification of targets in real time and the other concerned with voice recognition – the group was addressed by Yevgeny Maximov, deputy head of the FSB’s research establishment. Responsibility for both projects was given to the FSB and its director Alexander Bortnikov.
>
> Initially the question was formulated thus: Russia needs its own dynamic automated human identification system using ‘the texture and three dimensional forms of the facial surface’. In practice the task was understood more widely: the FSB invited tenders for systems that would use CCTV to pick out a potential criminal by his or her walk and facial expression, and combinations of factors revealing a person’s stress levels, and even included in their specification a programme module which would be capable of distinguishing between a living face and a mask or cast.[112]

One system being trialled in Moscow’s metro stations uses software that captures facial features and then compares that data with Interior Ministry databases. As the software’s founder notes, it can scan 10 million images in seven seconds and can “pinpoint a person’s whereabouts at a given moment with an accuracy of up to 96%.”[113] The whole system is expected to be rolled out throughout Moscow’s city streets, squares, airports, railway stations, and public transport, feeding a steady stream of data directly to operators who can check the images for an exact match.[114] Since 2020, this approach seems to have been embraced, with the authorities planning to expand the cameras throughout trams, underground railways, and outside apartment buildings and public spaces in various cities, including in the capital.[115]

[111] Ibid.
[112] Ibid.
[113] Ibid.
[114] Ibid.
[115] Human Rights Watch (2 October 2020) Russia expands facial recognition despite privacy concerns. Available at: https://www.hrw.org/news/2020/10/02/russia-expands-facial-recognition-despite-privacy-concerns [accessed 21 October 2020].

However, CCTV facial recognition technologies are still evolving, and they are presently far from flawless.[116] They are most accurate when a clear shot can be logged, but this is evidently more challenging with angular shots in streets or crowds.[117] As a Scotland Yard detective notes, "[at] the airport, if you go to the facial recognition machine, you want it to work, so you are looking dead at the camera … And yet it only works 90% of the time."[118] Nonetheless, the combination of high definition cameras, equipped with increasingly sophisticated facial recognition and behavioural software, feeding into live-stream networked security centres, means that counterintelligence can identify targets almost automatically and react with immediacy.[119] As Lord contends, 'they could effectively grant omniscience to counterintelligence personnel wherever they have placed cameras … Without an effective countermeasure, intelligence officers will be at risk of identification the moment they step out of their front door.'[120] Indeed, in an authorised experiment in China, one journalist attempted to travel unnoticed through the city of Guiyang, where it took only a matter of minutes before cameras identified the reporter and officers arrived at the scene.[121]

Further cause for concern is raised by advances in DNA analysis.[122] Many countries have now collated large DNA databases, typically of domestic citizens who commit serious crimes.[123] One country of particular note is China, which continues to

[116] Gates, K. A. *Our biometric future: facial recognition technology and the culture of surveillance*, (New York, New York University Press, 2011), p. 70-74.
[117] Ibid.
[118] BBC News (3 February 2015) Facial recognition technology: How well does it work? Available at: http://www.bbc.co.uk/news/technology-31112604 [accessed 11 January 2018].
[119] Lord, J. 'Undercover under threat', p. 686.
[120] Ibid.
[121] BBC News (10 December 2017) In your face: China's all-seeing state. Available at: http://www.bbc.co.uk/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state [accessed 11 January 2018].
[122] Inkster, N, 'Intelligence agencies', p. 45.
[123] As Asplen argues, '[as of 2014] the volume of [DNA] databases changes daily and probably by the thousands globally, the volume of DNA profiles is approximately 35 million records contained in forensic databases worldwide. Those countries with the largest databases are China, containing in excess of 12 million, the United States with more than 10.4 million, and the United Kingdom with more than 4.8 million'. For more details, see Asplen, C. 'DNA databases', *in Forensic DNA Applications: an*

pressure its citizens into providing DNA samples for an ever expanding network of databases, citizens who have often not been convicted or even suspected of crimes. This point is underscored by *Human Rights Watch*:

> [samples] have also been collected from vulnerable groups already targeted for increased government surveillance, including migrant workers, dissidents, and minority Muslim Uyghurs … [because] police wield wide powers, and because there are no actionable privacy rights in China, people have little ability to refuse the collection of such personal information.[124]

As the volume of DNA databases increase, this data can be cross examined with rapid advances in forensic testing, allowing people to be tied to a time and place with speed and precision.[125] For example, security specialists, in reference to ongoing issues with HUMINT cover, stated that the time taken to obtain DNA results has since decreased from weeks to hours, and is anticipated to take minutes within a decade.[126] Should that occur, DNA sequencing would be applicable en masse at airports and border crossings, adding a further level of risk to a traveller's alias.[127]

It also bears note that much of this information could be acquired before an operative even sets foot in Moscow or Beijing. As exemplified by the EU's Schengen area, many countries share biometric data, meaning a traveller's biometrics might already be on file in a country they had never visited.[128] They can also be acquired through illicit means. According to Wikileaks, the CIA siphoned biometric data from

---

Interdisciplinary Perspective, edited by Dragan Primorac and Moses Schanfield (Boca Raton, CRC Press, 2014), p. 559

[124] Human Rights Watch (15 May 2017) China: Police DNA Database Threatens Privacy. Available at: https://www.hrw.org/news/2017/05/15/china-police-dna-database-threatens-privacy [accessed 18 January 2021].

[125] Imam, J, et al 'DNA fingerprinting: discovery, advancements, and milestones', in *DNA Fingerprinting: Advancements and Future Endeavours,* edited by Hirak Ranjan Dash, Pankaj Shrivastava, Braja Kishore Mohapatra, and Surajit Das (Singapore, Springer, 2018), p. 21.

[126] Brannen, K. (6 April 2015) To catch a spy, *Foreign Policy.* Available at: http://foreignpolicy.com/2015/04/06/to-catch-a-spy-biometrics-cia-border-security/ [accessed 12 January 2018].

[127] Ibid.

[128] Gioe, D. 'The more things change', p. 216.

its own allies through an information sharing programme known as *ExpressLane*.[129] The programme was supposed to share biometric data with foreigner liaison agencies, but software updates installed by visiting CIA technicians secretly plundered additional biometric data those agencies had not agreed to share.[130] While the extent of the breach is unknown, media reports indicate that at least 1 billion Indian biometrics may have been compromised.[131] Similarly, Israel is so concerned abouts its intelligence officers' biometrics falling into the wrong hands, that it has barred their entry into a national biometric identity card trial.[132] The scheme builds upon on outdated 'Population Registry' which in 2006 was subjected to a major online leak, involving the online exposure of millions of Israelis' data.[133] The notion that states might target their opponent's biometrics is hardly novel, and the threat should be expected to rise parallel to their concurrent counterintelligence dividends.

In 2016, China raised the bar of such fears with the Office of Personnel Management hack, which included the theft of an estimated 1.1 million US federal employees' fingerprints.[134] As one former NSA officer noted, "[it's] perhaps the biggest counterintelligence threat in my lifetime … There's no situation we've had like this before, the compromise of our fingerprints. And it doesn't have any easy remedy or

[129] The Verge (24 August 2017) The CIA built a fake software update system to spy on intel partners. Available at: https://www.theverge.com/2017/8/24/16197694/cia-fake-software-update-hacking-WikiLeaks-vault-7 [accessed 11 January 2018].
[130] Wikileaks (24 August 2017) ExpressLane. Available at: https://wikileaks.org/vault7/#ExpressLane [accessed 04 August 2020].
[131] Chitra, R. (26 August 2017) WikiLeaks hints at CIA access to Adhaar data, officials deny it, *The Times of India.* Available at: https://timesofindia.indiatimes.com/india/WikiLeaks-hints-at-cia-access-to-aadhaar-data-officials-deny-it/articleshow/60228184.cms [accessed 11 January 2018].
[132] itNews (4 March 2014) Israeli spies banned from biometric ID cards, passports. Available at: https://www.itnews.com.au/news/israeli-spies-banned-from-biometric-id-cards-passports-373849 [accessed 11 January 2018].
[133] Lior, I. (3 March 2014) Shin Bet, Mossad bar employees from signing up for biometric database, *Haaretz*. Available at: http://www.haaretz.com/israel-news/.premium-1.577516 [accessed 11 January 2018].
[134] Scott, J. et al. 'Preparing the battlefield: The coming espionage culture post OPM breach', *Institute for Critical Infrastructure,* 2015, p. 16-17.

fix in the world of intelligence."[135] Fingerprints are used by the federal government for a variety of purposes, including accessing sensitive systems, but that data is now in the hands of Chinese counterintelligence.[136] Fortunately, CIA officers were not included in the breach as Langley holds its own records.[137] However, the theft could still leave contractors and federal employees exposed, people who may now be unable to pursue a career within the agency or engage with roles requiring defensible cover in China. Moreover, the absence of the CIA records could itself create complications, as Corera explains, 'a smart intelligence service could simply correlate who at an embassy was on the OPM database and, by process of elimination, work out that anyone not on the database was an undercover intelligence officer'.[138] This underscores a larger threat, with US experts concerned that Chinese security services are building a vast database of Americans, using information stolen through hacking.[139] These suspicions have been fed by anonymous CCP sources of the *Epoch Times,* who claimed that Chinese security services and technology companies are collating an enormous database of foreigners using data collected from covert activities.[140] Similar sentiments were expressed by US counterintelligence officials interviewed by *Los Angeles Times,* who claimed that '[foreign] spy services, especially in China and Russia, are aggressively aggregating and cross-indexing hacked U.S. computer databases – including security clearance

[135] Ibid.
[136] Ibid.
[137] Corera, G. (7 April 2016) The spies of tomorrow will need to love data, *Wired.* Available at: http://www.wired.co.uk/article/spies-data-mi6-cia-gordon-corera [accessed 11 January 2018].
[138] Ibid.
[139] Nakashima, E. (5 June 2015) With a series of major hacks, China builds a database on Americans, *The Washington Post.* Available at: https://www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fd-d580f1c5d44e_story.html?utm_term=.edb34ba1d249 [accessed 11 January 2018].
[140] Philipp, J. (1 March 2016) You're on file: Exclusive inside story on China's database of Americans, *The Epoch Times*. Available at: https://www.theepochtimes.com/youre-on-file-exclusive-inside-story-on-chinas-database-of-americans_1973047.html [accessed 11 January 2018].

applications, airline records and medical insurance forms'.[141] The article, supplemented by extensive interviews, adds:

> The Obama administration has scrambled to boost cyberdefenses for federal agencies and crucial infrastructure as foreign-based attacks have penetrated government websites and email systems, social media accounts and, most important, vast data troves containing Social Security numbers, financial information, medical records and other personal data on millions of Americans.
>
> Counterintelligence officials say their adversaries combine those immense data files and then employ sophisticated software to try to isolate disparate clues that can be used to identify and track — or worse, blackmail and recruit — U.S. intelligence operatives.[142]

According to US intelligence officials, a major source of concern is that China is combining data from OPM with millions of Americans' records acquired from other breaches, including travel information stolen from United Airlines, and health records stolen from Anthem. Russian hackers tied to the Kremlin have also been accused of hacking US State Department emails and financial companies, again to collect information on potential operatives.[143]

Compiling enormous portfolios on persons of interest is hardly exclusive to Russia or China. Indeed, Britain's Intelligence and Security Committee notes that GCHQ, MI5, and SIS all maintained 'bulk personal datasets' on targets of interest.[144] These are vast bodies of data that can be combined with analytical software, turning unintelligible information into useful and actionable results. [145] As SIS told Britain's Intelligence and Security Committee, bulk personal datasets "are increasingly used to identify the people that we believe that we have an interest in; and also to identify the

[141] Bennett, B. & Hennigan, W. J. (31 August 2015) China and Russia are using hacked data to target U.S. spies, officials say, *Los Angeles Times.* Available at: http://www.latimes.com/nation/la-na-cyber-spy-20150831-story.html [accessed 11 January 2018].
[142] Ibid.
[143] Ibid.
[144] Intelligence and Security Committee of Parliament, 'Privacy and security: a modern and transparent legal framework', *House of Commons,* 2015, p. 55.
[145] Corera, G. (7 April 2016) The spies of tomorrow will need to love data, *Wired.* Available at: http://www.wired.co.uk/article/spies-data-mi6-cia-gordon-corera [accessed 11 January 2018].

linkages between those individuals and the UK that we might be able to exploit".[146] But by compiling bulk personal datasets of their own, Russian and Chinese security services could expose undercover intelligence officers before they set foot in Moscow or Beijing.[147] As former NSA officer David Aitel argues, the flight patterns stolen in the United Airlines hack, especially those of operatives travelling to CIA headquarters in Langley, would be deeply revealing:

> "[every] CIA employee and visitor coming from abroad flies in and out of Dulles, and chances are they're flying United … [cross-referencing] names contained in the OPM, IRS and other caches would expose identities of US personnel working abroad under commercial or diplomatic cover".[148]

Cumulatively, these emerging and proliferating technologies call into question the long-term defensibility of cover aliases, increasing the odds of undercover travellers being identified and subjected to intensive street surveillance.

So far, proposed solutions are limited. One possibility, as Stein argues, is to manipulate foreign databases with human agents or hacking, to 'change data on demand'.[149] According to Bellingcat, Russia's FSB pursued a similar strategy in 2015, pressuring a source dubbed "Vadim" to manipulate UK visa systems.[150] The source, who worked for a company which offers IT services to the British consulate in Russia, claims to have been forced to create a backdoor into the visa network.[151] The Foreign Office denies claims that this is how the GRU operatives who poisoned the Skripals in 2018 gained visas to the UK, but it nonetheless reveals a foreign intelligence interest in

[146] Intelligence and Security Committee of Parliament, 'Privacy and security', p. 55.
[147] Business Insider (1 September 2015) Russia and China could be 'making it impossible for the US to hide' its intelligence activities. Available at: http://uk.businessinsider.com/russia-china-us-intelligence-database-2015-8 [accessed 11 January 2018].
[148] Ibid.
[149] Stein, J. (4 December 2012) CIA's secret fear: high-tech border checks will blow spies' cover, *Wired.* Available at: https://www.wired.com/2012/04/cia-spies-biometric-tech/ [accessed 11 January 2018].
[150] Bellingcat (16 November 2018) Spies without borders – how the FSB infiltrated the international visa system. Available at: https://www.bellingcat.com/news/uk-and-europe/2018/11/16/spies-without-borders-fsb-infiltrated-international-visa-system/ [accessed 10 July 2019].
[151] BBC News (16 November 2018) Russia 'sought access to UK visa issuing system'. Available at: https://www.bbc.co.uk/news/world-europe-46237634 [accessed 5 November 2020).

manipulating the immigration process, one that could be just as beneficial for SIS and the CIA.[152] Indeed, Langley seemed to have considered this option seriously, as one former CIA officer told *Wired*:

> "[just] before I left, they were gearing up to make a request for CIA to recruit foreigners with access to immigration databases … I'm sure that several people made careers out of just this kind of operation, much as some officers did when the NSA suddenly lost millions of access points to intelligence when the world switched from microwave towers to fiber optic lines – whole departments were formed to recruit telephone company assets in foreign countries."[153]

Alternatively, Streeter proposes injecting malware into foreign biometric systems, temporarily forcing counterintelligence to return to more primitive methods, a tactic that could be used the moment operatives arrive in a country, '[this] would be simple, clean, and as many authors testify, devastatingly effective.'[154] But even assuming these highly protected systems could be breached, there may be no way to know whether the event succeeded, posing serious risks, 'if they go wrong, the consequences could be disastrous'.[155] Moreover, to reiterate the point, solving one problem, such as biometrics, does not solve the myriad of other problems - successfully passing through a biometric checkpoint is only the first hurdle for today's operative.

Others have suggested reforms to cover itself. Lord, for example, argues that the intelligence community 'must overhaul the process by which it creates cover identities. Digital profiles must be manufactured in such a way that they blend better with those of real identities'.[156] Ross, on the other hand, advocates using only one alias per country, "[one] way biometrics can be overcome: don't go against the tide, swim with it … [so] long as countries are not sharing biometric information, one identity per country is one

[152] Ibid.
[153] Stein, J. (4 December 2012) CIA's secret fear: high-tech border checks will blow spies' cover, *Wired.* Available at: https://www.wired.com/2012/04/cia-spies-biometric-tech/ [accessed 11 January 2018].
[154] Streeter, D. C. 'Biometrics', p. 16-17.
[155] Lucas, E. *Spycraft rebooted,* see chapter 6.
[156] Lord, 'Undercover under threat', p. 686.

interim solution."[157] This approach is problematic, firstly because the sharing of biometric information means that intelligence officers may need to use a single identity in a group of countries, and secondly, because intelligence officers cannot guarantee whether that identity has been compromised by further sharing.[158] In a similar vein, Tucker suggests that intelligence officers might use their 'true name', a point reinforced by Inkster, "[the] days in which intelligence officers could plausibly adopt different identities and personas are pretty much coming to an end".[159] Using one's true name, however, means that once a person's intelligence affiliation is exposed (if an operation goes awry), then the operative is permanently blown. Furthermore, a "true name" brings a lifetime's worth of digital history, providing more clues as to the operative's background. Realistically, as one senior official acknowledges, Langley has to accept that's its operatives will "come in with digital dust and a digital background … There are very few Ted Kaczynskis living in a cabin up in the woods totally disconnected." [160] As a consequence, there is no simple fix - intelligence officers must assume the worst, and operate under the assumption that whether through biometrics or life history data, their identity is known to counterintelligence.

Cyberspace and the "golden opportunity".

The decline of defensible cover affects more than just undercover intelligence officers, for example, US officials are highly concerned that scientists and engineers who offer

[157] NewsRep (24 March 2015) How technology is changing the future of espionage. Available at: https://thenewsrep.com/40315/technology-changing-future-espionage/#ixzz3imhEq0HG [accessed 23 February 2018].
[158] Gioe, D. 'The more things change', p. 216.
[159] Tucker, D. *End of intelligence: Espionage and state power in the information age,* (Palo Alto, Stanford University Press, 2014), p. 83; Jones, S. (28 September 2016) The spy who liked me: Britain's changing secret service. *Financial Times.* Available at: https://www.ft.com/content/b239dc22-855c-11e6-a29c-6e7d9515ad15 [accessed 1 March 2018].
[160] Bloomberg (1 August 2016) CIA cyber official sees data flood as both godsend and danger. Available at: https://www.bloomberg.com/news/articles/2016-08-01/cia-cyber-official-sees-data-flood-as-both-godsend-and-danger [accessed 11 January 2018].

technical assistance in the field (and also rely on cover) might be identified and blackmailed.[161] But the clearest threat of all is that counterintelligence can identify undercover operatives with speed and precision, focusing their surveillance manpower accordingly.[162] Without reasonable alternatives, intelligence officers must operate under the assumption that they are being watched, turning to alternative tradecraft to reduce their dependency on increasingly dangerous personal meetings.[163] As noted in the literature review, intelligence agencies have developed a wide array of tradecraft tools over the centuries, but these are not sufficient to overcome the challenges detailed in this thesis.[164] This was demonstrated in 2015, when John Brennan announced sweeping reforms to the CIA, including the agency's first new directorate in fifty years, the Directorate of Digital Innovation (DDI).[165] Its purpose, as Brennan adds, is to "up" the CIA's "game", by researching and exploiting the full potential of digital technology.[166] In one sense, these changes aim to improve Langley's aging

[161] Bennett, B. & Hennigan, W. J. (31 August 2015) China and Russia are using hacked data to target U.S. spies, officials say, *Los Angeles Times.* Available at: http://www.latimes.com/nation/la-na-cyber-spy-20150831-story.html [accessed 11 January 2018].
[162] Clark, R. *Intelligence Collection*, p. 60-61.
[163] Gioe, D. V. 'The more things change', p. 217.
[164] See chapter 1.
[165] A second, and equally significant change is the combining of analysts and intelligence officers into single 'mission centres', in a move designed to improve efficiency. Originally, these two distinct functions were separated to avoid group think, but were later combined together in the War on Terror within the CIA's bustling Counterterrorism Center (CTC). The CTC has since become a model for operational divisions focused specifically on state-level threats, albeit the move has encountered some resistance, and some optimism, by former CIA officials. For more details, see Reuters (2 November 2016) Special report – John Brennan's attempt to lead the CIA into the age of cyberwar. Available at: https://uk.reuters.com/article/uk-usa-cia-brennan-specialreport/special-report-john-brennans-attempt-to-lead-the-cia-into-the-age-of-cyberwar-idUKKBN12X1L2 [accessed 11 January 2018]; Defense One (6 March 2015) CIA restructuring adds new cyber focus. Available at: http://www.defenseone.com/technology/2015/03/cia-restructuring-adds-new-cyber-focus/106953/ [accessed 11 January 2018]; Slick, S. (4 May 2016) Measuring change at the CIA, *Foreign Policy.* Available at: http://foreignpolicy.com/2016/05/04/measuring-change-at-the-cia/ [accessed 11 January 2018]; FCW (1 October 2015) Inside the CIA's new digital directorate. Available at: https://fcw.com/Articles/2015/10/01/CIA-digital-directorate.aspx?Page=1 [accessed 11 January 2018].
[166] Reuters (2 November 2016) Special report – John Brennan's attempt to lead the CIA into the age of cyberwar. Available at: https://uk.reuters.com/article/uk-usa-cia-brennan-specialreport/special-report-john-brennans-attempt-to-lead-the-cia-into-the-age-of-cyberwar-idUKKBN12X1L2 [accessed 11 January 2018].

infrastructure, including its networks, systems and databases.[167] As former CIA officer Stephen Slick claims, "[for] security, cultural, and occasionally budgetary reasons, it's safe to say CIA was never at or even near the cutting edge in information technology".[168] The CIA's former Deputy Director, David S. Cohen, notes that this is about more than just 'resistance to change':

> … what organization doesn't have to adapt to the digital world? — it's a much more complicated proposition for CIA. For example, as proud as we are of the cutting-edge clandestine technology we've developed for use in the field, our officers still can't bring smartphones into work, and we've only recently figured out how to allow some personnel to take notes in a meeting on a laptop instead of with a pen and paper.
>
> This isn't simply resistance to change. As an intelligence agency working with our country's most sensitive secrets, we need to operate in a secure environment, protected from the prying eyes of hostile intelligence services. That considerably complicates how we operate in the digital domain.[169]

Hence, as noted by its new director, one of the digital directorate's first aims is to 'aggressively retire' this outdated infrastructure, or 'legacy systems'.[170] The DDI will also acquire new data analytics software, through partnerships with the private sector,

[167] FCW (1 October 2015) Inside the CIA's new digital directorate. Available at: https://fcw.com/Articles/2015/10/01/CIA-digital-directorate.aspx?Page=1 [accessed 11 January 2018].
[168] Ferris paints a bleak picture of early CIA involvement with cyberspace, '[merely] to send intranet e-mail to intelligence officers outside the agency was difficult. Few CIA computers were linked to the SIPRnet [US classified networks]– though models which could receive but not send messages were quickly being introduced.' The main issue stemmed to CIA material being disseminated beyond its control, leading headquarters to tightly control how information could be spread or received within internal and wider networks. As Bruce Berkowitz added "the CIA's approach is not 'risk management' but 'risk exclusion'. All this had cultural causes and consequences. Access by outsiders to CIA data threatened its hierarchical system of assessment and quality control, while by making technology a bogey-man rather than an ally, the CIA is reinforcing the well-known tendency toward introversion among most DI [Directorate of Intelligence] analysts". Ibid; Ferris, J. 'Netcentric warfare, C4ISR and information operations: towards a revolution in military intelligence?', in *Understanding Intelligence in the Twenty-First Century, edited by L. V. Scott and P. D. Jacking'*, (London, Routledge, 2004), p. 54-77; Berkowitz, B. 'The DI and "IT": Failing to keep up with the information revolution', *Studies in Intelligence, CIA,* 74:1, 2003, p. 67-74.
[169] CIA (18 September 2015) Deputy Director Cohen delivers remarks on CIA of the future at Cornell University. Available at: https://www.cia.gov/news-information/speeches-testimony/2015-speeches-testimony/deputy-director-cohen-delivers-remarks-on-cia-of-the-future-at-cornell-university.html [accessed 10 January 2018]
[170] FCW (1 October 2015) Inside the CIA's new digital directorate. Available at: https://fcw.com/Articles/2015/10/01/CIA-digital-directorate.aspx?Page=1 [accessed 11 January 2018].

to improve intelligence analysis.[171] As Cohen explains, 'these DDI data scientists will develop and deploy customized IT tools to help our analysts make connections in the data and test the analytic calls they make', adding, '…the variety, complexity and volume of data we take in … calls for some of the most sophisticated and cutting-edge programming and "big data" analysis being performed anywhere today.'[172] But despite these supporting functions, the DDI's focus is very much centred on counterbalancing the threats to intelligence officers' cover, by understanding the threats and opportunities technology brings.[173] In a 2016 interview with the *Aspens Institute*, Brennan elaborated on the directorate's purpose, "[we] established the digital directorate because that digital environment affects our profession, just the way that it affects everybody's lives, and so how we operate around the world". He added:

> … the digital directorate … has responsibility not just for protecting our systems, and networks, and databases, but also being able to understand all the implications of that digital environment … now with all the biometrics that are out there, and the CCTV's that are out there, as well as anytime you use your ATM , or you use your credit card, you create digital dust, and we all have forensic history that we continuing to accrue every day …
>
> We need to make sure that their forensic history, their digital history, matches their cover legend … that's just one example of [how] this digital environment has fundamentally affected our ability to carry out our work. And so this digital [directorate] is the one that has responsibility to be thinking about what are the risks, what are the threats, what are the challenges, but also what are the opportunities? And I think for too long the intelligence community was pushing off technology and saying no, we need to stay clear of it.[174]

[171] Defense One (1 October 2015) Meet the man reinventing CIA for the big data era. Available at: http://www.defenseone.com/technology/2015/10/meet-man-reinventing-cia-big-data-era/122453/ [accessed 11 January 2018].
[172] CIA (18 September 2015) Deputy Director Cohen delivers remarks on CIA of the future at Cornell University. Available at: https://www.cia.gov/news-information/speeches-testimony/2015-speeches-testimony/deputy-director-cohen-delivers-remarks-on-cia-of-the-future-at-cornell-university.html [accessed 10 January 2018]
[173] The Aspen Institute (29 July 2016) A candid conversation with the Director of the Central Intelligence Agency, *Youtube*. Available at: https://www.youtube.com/watch?v=TRCUO7-lbUE [accessed 11 January 2018].
[174] Ibid.

This notion that digital and cyber technology must be understood for espionage purposes is accepted throughout the global intelligence community, with technology deemed a driver for SIS's substantial increase in funding (upping its personnel by forty percent).[175] As the *Financial Times* writes, UK intelligence officials believe that these technological threats demand 'more fulsome changes to the very nature of spycraft itself'.[176] In a joint 2018 interview with his American and Australian counterparts, the chief of SIS, Alex Younger, claimed that technology was "fundamentally" changing the "operating environment", adding "in five years' time, there will be two sorts of intelligence services, those that understand this fact and have prospered, and those that don't and haven't. And I'm determined that MI6 will be in the former category."[177] However, he added that while espionage is increasingly threatened by technology, cyberspace also offers a "golden opportunity":

> …cyber is still another form of human interaction – it's got human beings at the other end of it. But it represents a whole set of new disciplines. For us in the UK, it's led to a significant … integration of the technical intelligence world, and the human intelligence world … the nexus of technology and human intelligence actually is a big part of our future. So I think this a fabulously important issue, and one, as I say, that will dictate our future success.[178]

This point was reinforced by Australia's ASIS chief, Nick Warner, who added that intelligence agencies will either have to change how they do business, or "fail".[179] While serving intelligence officers avoid specifying what these changes might look like, it is clear from the literature review that many former practitioners see cyberspace

[175] BBC News (21 September 2016) MI6 set to recruit 1,000 extra staff. Available at: http://www.bbc.co.uk/news/uk-37434131 [accessed 10 January 2018].
[176] Jones, S. (28 September 2016) The spy who liked me: Britain's changing secret service. *Financial Times.* Available at: https://www.ft.com/content/b239dc22-855c-11e6-a29c-6e7d9515ad15 [accessed 1 March 2018].
[177] GW Center for Cyber and Homeland Security (21 September 2016) CIA-GW intelligence conference: Panel on the view from foreign intelligence chiefs, *Youtube*. Available at: https://www.youtube.com/watch?v=yefBv7Q3sv0 [accessed 11 January 2018].
[178] Ibid.
[179] Ibid.

as an avenue to upgrading tradecraft and achieving operational success. Consequently, the merits of cyberspace, that remain opaque, are indelibly tied with the West's ability to operate and succeed within these hard target states.

Evaluation

In summary, if espionage is to succeed in Russia and China, it must adapt to the reality of this profound street surveillance threat. It is clear that both regimes regard surveillance as a crucial barrier against clandestine operations. Although the Kremlin's rhetoric against outside interference is in part a means of delegitimising Putin's political opponents, it is also evident that the Kremlin regards foreign spying as a pivotal threat. Consequently, the FSB has grown into one of the largest security services in the world, with a manpower in the hundreds of thousands. Likewise, President Xi's regime, which regards almost all foreigners with suspicion, has bolstered its vast security services through its new Counterespionage Law, a sign that its tolerance for espionage is swiftly declining. In both cases, tight travel restrictions on government and defence officials ensures that the most attractive quarry are contained into tightly surveilled spaces such as Moscow and Beijing. And any operatives who wish to compete here must account for a rising trend of hostility, wherein they face not just observation, but outright harassment and assault.

While these conditions are naturally unfavourable, technology adds a further dimension to the problem. The most immediate challenge is the proliferation of biometric scanners in airports and border crossings, which threaten to permanently tie an intelligence officer's identity to their biometric passports. These scanners, that operate at near-perfect efficiency, cannot be easily fooled, nor can they be easily avoided. Furthermore, if a travelling intelligence officer's biometrics are flagged, they

will highly likely be pulled aside for secondary screening, where a more invasive investigation may follow. Herein, counterintelligence officers will face few problems comparing the operative's alleged cover story against their online background. The absence of the kind of digital history associated with today's interconnected professionals would naturally cause suspicions, and yet too much information could potentially lead to gaps in the operative's memory. As a consequence, there is no perfect system for ensuring a defensible cover.

The widespread use of CCTV cameras and advances in DNA testing, only adds further cause for concern. It is evident that Russian and Chinese security services have sought to incorporate interconnected, advanced CCTV networks within their surveillance apparatus. These systems, combined with facial recognition capabilities, can follow operatives as they move throughout transport systems and public spaces, offering few safe harbours for privacy. Even if an intelligence officer successfully loses their 'tail', they cannot escape the pervasive glare of smart cameras, allowing surveillance teams to lock onto their targets and arrive at the scene within a matter of minutes. Combined, these factors allow surveillance teams to track undercover targets with speed and precision, leaving few places to hide.

Much of this evidence can be gathered before operatives set foot in the target country, as demonstrated through the reported acquirement and collation of enormous personal information datasets. The vast vetting records stolen from the US Office of Personnel Management, underscores Russia and China's increased willingness to pursue these datasets through any means at their disposal. The OPM hack, when combined with other major breaches like United Airlines and Anthem, have put enormous amounts of personally exposing information into the hands of foreign counterintelligence, data which could easily pierce an intelligence officer's cover from

the moment they set foot in an airport. Thus, despite being an age increasingly defined by the mass movement of people, it is proving exceptionally difficult for intelligence officers to seamlessly travel in key environments.

Solutions to these problems remain slim. Despite suggestions that biometric databases or visa systems can be tampered with, these are likely to be heavily defended, and no attempt to do so offers guaranteed results. Alternatively, intelligence officers can travel into these countries either using their real identities, or one persistent cover applied to a group of countries, a solution which leaves no room for mistakes. If an operative under a single-use cover is compromised, then they cannot return to the same country under a new identity, permanently barring them from the operational theatre. More to the point, single use identities are not guaranteed to be reliable, since the sharing of data between countries means an operative's actions in one country can lead to their exposure in another. As such, intelligence officers must come to terms with this new reality, and operate under the assumption that a single mistake could put an end to their regional career, or endanger their operations.

Against the spectre of technologically-enabled street surveillance, which is unlikely to dissipate in the foreseeable future, it is understandable that intelligence agencies are pursuing new means to recruit and handle agents. As revealed through the statements of senior officials, including the then serving heads of SIS and the CIA, and as illustrated in the creation of the CIA's first new directorate in over fifty years, cyberspace is now regarded as the solution to espionage's needs. But while intelligence chiefs view technology as a "golden opportunity", the benefits of cyber-enabled tradecraft are yet to be determined. Therefore, this chapter has established why cyber-enabled tradecraft may be critical to meeting espionage's hard target obligations, as a potential solution to a surveillance problem that cannot be ignored.

Chapter 4
Lessons from the KGB's panopticon.

Introduction

The previous chapter addressed the need for tradecraft modernisation to pierce two hard target regimes. This chapter provides a conceptual framework that allows the strengths and weaknesses of any proposed technological solution to be assessed, including cyberspace. This process of abduction, as proposed in the methodology, uses history to comprehend and predict the unobservable. This chapter thus holds two purposes. First, it assesses the argument for using espionage in the mid-late Cold War as a suitable, and relevant, historical case study. Second, it narrows the lens to the four functions of tradecraft – recruitment, surveillance, handling, collection – examining the various tools and techniques within these categories for underlying themes, in order to produce an abductive lesson. In drawing parallels between the Cold War and modern surveillance threats, it examines how the KGB constructed the perfect panopticon, as a means of suppressing internal dissent and thwarting foreign espionage. The West responded to this challenge with innovation, investing huge sums of money to technologically enhance their tradecraft. But despite some successes, overall, the rewards of this period were few and far between, marked by the recruitment of only a handful of high ranking Soviet spies, and fewer still who operated safely in Moscow. It argues that these events, as disclosed by a growing body of literature, offer an ideal starting point for further research. They are defined by struggle and loss, and thus rich in analytical value.

The lens is then narrowed to the various function of tradecraft, with attention focused on the evolution and limitations of espionage in this era. In order to produce holistic lessons, the approach taken here is broad, examining the limitations not just of

technology, but of tradecraft as a whole. However, since technology was applied in this era to compensate for the weaknesses of conventional tradecraft, key technological developments draw particular scrutiny; these include the telephone in recruitment, listening devices in surveillance, burst radio transmitters in handling, and subminiature spy cameras in collection. This chapter argues that while technology evolved, human behaviour played a pivotal role in determining its overall success, pushing up the need to develop trust under strenuous conditions.

The case for the Cold War

The first primary area of relevance pertains to the hostile counterintelligence conditions which necessitated, and obstructed, tradecraft of the era. In uncanny parallel to present circumstances, the KGB's surveillance systems offered few places for even the most determined of intelligence officers to hide.[1] Intensive surveillance was integrated into KGB ideology, primarily as means to suppress dissent and control the Soviet populace.[2] The scope of such control was Orwellian by design, with the entire USSR dissected into controlled zones, each with restricted freedoms of movement and networks of informants.[3] Practically every apartment block held a "director of the house", a combination of 'spy, concierge, janitor, rent collector, and apartment manager', who reported the daily affairs of tenants and visitors.[4] To maintain this level of pervasive control and monitoring, only a handful of citizens were given internal travel passports, without which free movement across the country was impossible.[5] Without these passports, Soviets could not leave their respective zones, could not acquire jobs in other

[1] Wallace, R. et al. *Spycraft: inside the CIA's top secret spy lab,* (London, Bantam Press, 2008), p. 51-53.
[2] Barron, J. *KGB: the secret work of Soviet secret agents* (New York, Bantam Books, 1974), p. 121-131.
[3] Ibid, p. 131-135.
[4] Ibid, p. 131
[5] Ibid, p. 134.

cities, and, if travelling for more than 72 hours, had to register their passports with local militia, subjecting an entire populace to surveillance.[6]

Moreover, Soviet citizens could only travel abroad if granted special permission by the KGB, where even the exceptions were often subjected to controls, monitoring, and restricted interaction with foreign nationals.[7] Those with access to state secrets were usually denied such privileges, or their children were forced to remain in the Soviet Union to deter parents from defection.[8] Stringent rules were also in place for outsiders, including tight controls over immigration. Khrushchev's regime eventually relaxed the USSR's intake of foreigners (compared to tight restrictions under Stalin), but overall immigration to the Soviet Union remained miniscule compared to Western countries.[9] Those permitted to enter could expect severe travel restrictions and surveillance, and were segregated from the populace at large.[10] In fact, foreigners were compacted into restricted spaces with access to only a handful of major cities, in particular Moscow.[11] Such measures remained throughout the Cold War – they survived six regime changes and, as one CIA report lamented, they went 'well beyond' those of any other country, even within the Eastern Bloc. [12]

These systems thus forced all foreigners, particularly those likely to be intelligence officers (diplomats and businessmen) into contained spaces, making

---

[6] Ibid.
[7] Feldbrugge, F. J. M. *Russian law: the end of the Soviet system and the role of law,* (Dordrecht, Martinus Nijhoff Publishers, 1993), p. 226; Soldatov, A. & Borogan, I. *The red web: the struggle between Russia's digital dictators and the new online revolutionaries,* [Kindle version] (New York, Public Affairs, 2015). Accessed 1 January 2018, see chapter 1.
[8] Andrew, C. & Mitrokhin, V. *The Mitrokhin archive: the KGB in Europe and the West* (London, Penguin Books, 2000), p. 845-846; Hutchings, R. *Soviet secrecy and non-secrecy,* (London, MacMillan Press, 1987), p. 181-182; Clarridge, D. R & Diehl, D. *A spy for all seasons: my life in the CIA,* [Kindle version] (New York, Scribner, 1997). Accessed 1 January 2018, p. 127-128.
[9] Matthews, M. *Party, state, and citizen in the Soviet Union: a collection of documents,* (London, M. E. Sharpe, 1989), p. xxviii-xxix.
[10] Ibid.
[11] CIA (22 December 2016) Restrictions on foreign travel in the USSR: Assessing recent changes. Available at: https://www.cia.gov/library/readingroom/docs/CIA-RDP07C00121R001000280001-8.pdf [accessed 1 January 2018].
[12] Ibid.

routine surveillance considerably more efficient. As such, CIA and MI6 officers adopted a set of unofficial guidelines, known as the Moscow Rules, that dictated the exceptional codes of conduct required to operate in the KGB's panopticon.[13] Moscow Rules have become something of a moniker for the challenges of operating in hard-target conditions, and they reflect the degree of vigilance required to stay secure under the KGB's umbrella. They include, but are not limited to:

1. Assume nothing.
2. Never go against your gut.
3. Everyone is potentially under opposition control.
4. Don't look back; you are never completely alone.
5. Go with the flow, blend in.
6. Vary your pattern and stay within your cover.
7. Lull them into a sense of complacency.
8. Don't harass the opposition.
9. Pick the time and place for action.
10. Keep your options open.[14]

Antonio Mendez, a CIA officer based in Moscow during the mid-1970s, notes how Moscow Rules were rarely ever taken for granted, especially Rule 1 – Assume nothing.[15] In fact, this rule may have been better written as *assume nothing but the worst*, since KBG surveillance teams were presumed to be everywhere. As one CIA officer stressed to Mendez "[assume] every Soviet you encounter is connected to a larger surveillance apparatus", candidly adding:

> This includes the women shoveling snow in the winter and the guy selling ice cream in Gorky Park. The ticket-taker at the zoo reports to the KGB. The bartenders in every hard-currency bar and restaurant are on the payroll of the Seventh Chief Directorate. Half the taxis in this part of the city are driven by their men."[16]

[13] Mendez, A. J. & McConnell, M. *The master of disguise: my secret life in the CIA*, [Kindle version] (New York, Harper Collins, 2007). Accessed 1 January 2018, p. 221-225.
[14] Spy Museum – Moscow Rules. Available at: https://www.spymuseum.org/exhibition-experiences/online-exhibits/argo-exposed/moscow-rules/ [accessed 1 December 2017].
[15] Mendez, A. J. & McConnell, M. *The master of disguise*, p. 204-206.
[16] Ibid, p. 204.

Once the KGB suspected someone of being an intelligence officer (especially if linked to the US, UK, or other NATO countries), they tasked a 'dedicated team' who focused their entire attention on that person 'twenty-four hours a day'.[17] In addition to being pursued by these teams (alongside informants and mobile support units) foreigners were directed to specific hotel rooms bugged with permanent listening devices, while surveillance units tapped living quarters and apartment blocks around-the-clock.[18] Consequently, the KGB cultivated the ultimate panopticon, where active surveillance was considered the norm rather than exception - as one CIA officer remarked, they assumed "constant surveillance" at all times.[19]

KGB surveillance machinery placed strains on conventional tradecraft, strains that became untenable by the time MI6 and the CIA recruited GRU colonel, Oleg Penkovsky.[20] Penkovsky was an invaluable agent, and yet surveillance mired his entire operation.[21] Because he was recruited in difficult circumstances and one of the first valuable agents to be handled in Moscow conditions, his tradecraft has drawn considerable study.[22] What is clear, however, is that by the time of his arrest, the KGB had observed multiple aspects of his ostensibly covert tradecraft, amassing a wealth of evidence later used in his highly publicised trial and cutting his espionage career

[17] Ibid, p. 205.
[18] Dulles, A. W. *The craft of intelligence: America's legendary spy master on the fundamentals of intelligence gathering for a free world*, (New York, The Lyons Press, 2006), p. 63' Mendez, A. J. & McConnell, M. *The master of disguise*, p. 221-226
[19] Mendez, A. J. & McConnell, M. *The master of disguise*, p. 204.
[20] Wallace, R. et al. *Spycraft*, p. 52,
[21] Penkovsky, O. *The Penkovsky papers: the Russian who spied for the West,* (London, Collins, 1967), p. 213.
[22] For key literature, see: Gioe, D. 'Handling HERO: joint Anglo-American tradecraft in the case of Oleg Penkovsky', in *An International History of the Cuban Missile Crisis*, edited by David Gioe, Len Scott, & Christopher Andrew, (London, Routledge, 2014); Duns, J. *Dead drop: the true story of Oleg Penkovsky and the Cold War's most dangerous operation,* [Kindle version] (London, Simon & Schuster, 2013). Accessed 21 June 2020; Corera, G. *The art of betrayal: life and death in the British secret service,* [Kindle version] (London, Weidenfeld & Nicolson, 2011). Accessed 12 May 2020; Ashley, C. *CIA spymaster* (Gretna, Pelican Publishing Company, 2004).

short.[23] As Wallace et al, explain, his brief success depended more upon fortune rather than any sophisticated tradecraft, eventually leading Langley to rethink, and redesign, its operational repertoire:

> Technology did little to enhance either Penkovsky's production or security. His remarkable success was achieved not because of technology, but despite the lack of it. His official position allowed him periodic travel outside the USSR and opportunities for extensive debriefings. Without these personal meetings, Penkovsky would not have been successful.
>
> What became clear was that the CIA in the 1960s did not have the operational methodology, clandestine hardware, or personnel to run secure agent operations inside the USSR. The absence of secure and clandestine means of communicating in Moscow forced both the agent and his handlers to take risks that eventually played into the hands of the KGB surveillance methods. The recruitment of agents inside the Soviet Union meant little if the KGB could quickly identify them or if they could not securely communicate the secrets to which they had access.[24]

Until this point, technology in spy work had played only a minor role, offering little reprieve against Soviet surveillance. Developments had occurred in the Second World War, but such advances – including secret inks and mobile radio sets – were developed for warfare conditions, not for peacetime espionage in an Orwellian surveillance state.[25] They were 'too big, too cumbersome, too unreliable, too complex, and too power hungry … [in] the decidedly blunt terminology of one scientist of the day, the equipment was "junk."'[26] But Penkovsky's arrest coincided with the "scientific-technical revolution" of the 1960's (comparable to today's rapid advancements),

---

[23] The KGB even stationed teams above and across the river from Penkovsky's own home, to hone their observation. For more details, see CIA (2013) The capture and execution of Colonel Penkovsky, 1963. Available at: https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/colonel-penkovsky.html [accessed 1 January 2018]; Duns, J. *Dead drop*, see chapter 14.

[24] Wallace, R. et al. *Spycraft*, p. 39

[25] Jeffrey, K. *MI6: the history of the Secret Intelligence Service 1909-1949* (London, Bloomsbury, 2011), p. 628-629; Macrakis, *Prisoners, lovers, & spies: the story of invisible ink from Herodotus to al-Qaeda*, (New Haven, Yale University Press, 2014), p. 12-13; Kahn, D. *The codebreakers: the story of secret writing*, (New York, Scribner, 1996), p. 247-249 Lett, B. *SOE's mastermind: the authorised biography of Major General Sir Colin Gubbins*, (Barnsley, Pen & Sword Books, 2016), p. 156.

[26] For instance, SOE radios built for use behind enemy lines were highly vulnerable to detection if used for anything other than short messages, and consistently broke down (which the agents were responsible for fixing). As Lett elaborates, during the Second World War the 'detection and 'waste' rate of radio operations in the field was abnormally high', at least until more efficient radio sets were devised. For more information, see Lett, B. *SOE's mastermind*, p. 156; Wallace, R. et al. *Spycraft*, p. 52.

exemplified by 'big technology' programmes including the U-2 spy plane and Corona IMINT satellites.[27] In light of these achievements, a 'growing cadre' of CIA officers began to question whether the same advances which had placed intelligence in space, could be applied to the streets of Moscow.[28] As Macrakis contends, through the aid of a booming industrial base, technology was soon turned towards espionage:

> …by the time of the Cold War, technology had become a cure-all, a "fix" for numerous problems. Therefore, it should be no surprise that technological solutions were also applied to the intelligence problem of a closed society. The rise of the military-industrial-academic complex and growing technical capabilities during the 1950s facilitated this development.[29]

While the CIA had already developed a technical-industrial base through its Directorate of Science & Technology - the directorate responsible for larger, technical-gathering programmes such as the Corona satellites - by 1962 it had established a technical body specifically for creating new tradecraft solutions.[30] Known as the *Technical Services Division*, and later renamed the *Office of Technical Services*, this body was substantially expanded in the wake of Penkovsky's capture, in an effort to exploit emerging scientific possibilities. Over the following years, hundreds of scientists, engineers, and specialists were drafted into Langley's fold for a singular purpose, to develop cutting-edge tradecraft for use in the field.[31]

According to Wallace et al, rapid integration of technology into espionage affairs faced several challenges.[32] On the one hand, demands for security, particularly compartmentalisation, isolated technical specialists from key operational details. As one CIA officer lamented, "to perform the task perfectly the tech should know

[27] Macrakis, K. 'Technophilic hubris and espionage styles during the Cold War', *Isis,* 101:2, 2010, p. 378.
[28] Wallace, R. et al. *Spycraft,* p. 52.
[29] Macrakis, 'Technophilic hubris', p. 380.
[30] Wallace, R. et al. *Spycraft,* p. 53-57.
[31] Ibid.
[32] Ibid.

everything. But in our world the techs weren't allowed to know everything."[33] Culture also proved problematic, as intelligence officers, who were front and centre of operations and often steeped in tradition, viewed personal meetings, not 'spy gear', as the baseline for effective espionage.[34] But even as these cultural barriers eroded, the requirements placed on TSD often outstripped its resources, pushing up demand for outsider expertise, including universities, manufacturers, and even craftsmen who built intricate spy gear in their garages.[35] As such, upgrading espionage required more than a simple transition, and the fact that these cultural and organisational shifts occurred reflected the CIA's need for better tradecraft.

The CIA was quick to modernise its tradecraft in line with emerging scientific and technological advances throughout society, and it set a path that was followed by spy agencies on a global level.[36] Thus, the 1960's marked a turning point for espionage, including in Eastern Bloc nations, where technology became an 'active staple of practical spy work' (albeit with 'some time lag' behind the west).[37] Peter Wright's controversial MI5 exposé, *Spycatcher*, alludes to similar reforms taking place within British intelligence, including SIS.[38] During the early years of the Cold War, SIS controlled its own technical facilities (including elements absorbed from SOE), yet relied on outside scientific support.[39] Toward the late 1950s, however, it became evident that '[both] MI5 and MI6 needed their own establishments, their own budgets,

[33] Ibid.
[34] Ibid.
[35] Ibid.
[36] Macrakis, K. *Seduced by secrets: inside the Stasi's spy-tech world,* [Kindle version] (Cambridge, Cambridge University Press, 2008), p. 147.
[37] Ibid.
[38] It should be noted that while some of Wright's more profound claims about moles inside MI5 are largely considered to be untrue, his operational insights have been treated as factual. For example, writing in *Defence of the Realm,* Christopher Andrew uses some of *Spycatcher's* materials, including Wright's claims regarding technical surveillance. For more details, see Wright, P. & Greenglass, P. *Spycatcher*, (New York, Viking Penguin Inc, 1987), p. 167-168; Andrew, C. Defence of the realm, [Kindle version] (London, Penguin Books, 2010). Accessed 10 January 2018, section D, introduction.
[39] Davies, P. H. J. *MI6 and the machinery of spying,* (London, Frank Cass, 2004), p. 208-209

and their own staffs' for the purpose of researching and developing technological tradecraft.[40] This led to the transformation of a former SIS agent communications centre into a tradecraft research division for both SIS and MI5, as Davies elaborates:

> Since both SIS and the Security Service had essentially similar requirements for research and development, and both were prevented by considerations of security and specialised needs from acquiring the bulk of their technology on the open market, there existed both administrative and productive economies of scale in pooling their research and development programmes.
>
> James Adams has asserted that basically the SIS needs these developments to perform espionage and that MI5 is developing counter-measures should the same techniques be employed against the UK by an adversary, but this reality oversimplifies the situation. Since the SIS is responsible for counter-intelligence and security abroad, while the Security Service collects intelligence in the UK, both services have a percentage in developing both offensive techniques and counter-measures for use in their respective jurisdictions.[41]

In addition, this expansion drew scientists from the wider Civil Service, breaking down artificial barriers between SIS and the British scientific community.[42] Thus, at least for Western intelligence services, the 1960s marked the point when scientific advances, combined with growing demand for innovative solutions to the Moscow problem, instigated an evolution of tradecraft at both the operational and cultural level, redefining attitudes towards technology in espionage.

Through these developments, technology became an embedded feature of Moscow Rules, but while advances in tradecraft opened new opportunities, intelligence officers fell short of their overall objectives.[43] Tradecraft reforms ran parallel to the procurement of various valued agents in the mid-late years of the era, most notably Dmitry Polyakov, Adolf Tolkachev, Ryszard Kuklinski, Alexander Ogorodnik, and

[40] Wright, P. & Greenglass, P. *Spycatcher*, p. 167-168
[41] Davies, P. H. J. *MI6 and the machinery of spying*, p. 265.
[42] Wright, P. & Greenglass, P. *Spycatcher*, p. 167-168
[43] Mendez, A. et al. *The Moscow rules: the secret CIA tactics that helped America win the Cold War*, (New York, Public Affairs, 2019), p. 20-21; Russel, R. L. *Sharpening strategic intelligence: why the CIA gets it wrong and what needs to be done to get it right*, [Kindle version] (New York, Cambridge University Press, 2007), p.51-52

Oleg Gordievsky.[44] Yet, these significant achievements were tempered by an almost total failure to penetrate the upper echelons of Soviet leadership.[45] As the former Director of the CIA, Robert Gates, protested, "[we] never recruited a spy who gave us unique political information from inside the Kremlin, and we too often failed to penetrate the inner circle of Soviet surrogate leaders."[46] Even with improved capabilities the CIA and SIS struggled to identify and cultivate potential agents on their own terms, leading to a high dependency on Soviet officials who willingly volunteered their services (known as walk-ins), a point candidly underscored by ex-CIA senior operations officer, Duane Clarridge:

> Historically, those who really wanted to cooperate with the United States have walked in of their own volition and offered their services, usually for money. I know of no significant Soviet recruitment that was spotted, developed, and recruited from scratch by a CIA case officer.[47]

But owing to a restricted ability to conduct operations inside Soviet territory, this overreliance on volunteers ran parallel to a dependency on sources who travelled abroad.[48] As such, only a handful of high valued agents were recruited in the mid-late Cold War, almost all of whom were eventually betrayed by moles Edward Lee Howard, Aldrich Ames, and Robert Hanssen.[49] As Ames conceded, he'd given the KGB the names of "virtually all Soviet agents of the CIA and other American and foreign services" known to him, a striking admission, given his assigned position offered access to virtually all major US operations within the Soviet Union.[50] The list of known Soviet assets betrayed by the trio are as follows:

Boris Yuzhin, sentenced to six years in the Gulag

[44] Mendez, A. et al. *The Moscow rules*, p. 174.
[45] Russel, R. L. *Sharpening strategic intelligence,* p. 51-52
[46] Ibid.
[47] Clarridge, D. R & Diehl, D. *A spy for all seasons*, p. 124.
[48] Garthoff, R. L. *A journey through the Cold War: a memoir of containment and coexistence,* (Washington, Brookings Institution Press, 2001), p. 104.
[49] Wise, D. *Spy: the inside story of how the FBI's Robert Hanssen betrayed America*, (New York, Random House, 2002), p. 52
[50] Ibid.

Adolf Tolkachev, civilian, executed
Vladimir Mikhailovich Vasilyev, GRU colonel, executed
Dmitriy Fedorivich Polyakov, GRU general, executed.
Valery F. Martynov, KGB lieutenant colonel, executed.
Sergei Motorin, KGB major, executed.
Vladimir M. Piguzov, KGB, lieutenant colonel, executed.
Sergei Vorontsov, GRU lieutenant colonel, executed.
Gennady Smetanin, GRU lieutenant colonel, executed.
Gennady Grigorievich Varanik, KGB, executed.
Leonid Polyshuk, KGB, executed.
Vladimir V. Potashov, escaped.
Sergei Fedorenko, escaped
Sergei Bokhan, escaped
Oleg Gordievsky, KGB, escaped.[51]

This relatively small list embodied the bulk of the West's most valued Soviet agents, and yet, it also serves as a convenience for this thesis. Any study of tradecraft is very much a study of details, which requires substantive literature. But aided by the passage of official embargoes, increased openness of former practitioners, and the fact that these agents are now in the public domain, there is growing academic interest in the accomplishments, struggles, and tradecraft of this era.[52]

However, while the literature is dense with tradecraft generalisations, only a handful of specific cases demonstrate the full complexities of tradecraft in hard target conditions. Since most agents were recruited and handled in friendly territory, where

[51] Mendez, A. et al. *The Moscow rules*, p. 174.
[52] This includes two bodies of work written on the accomplishments and contributions of CIA's Office of Technical Services. First, *Spycraft*, co-authored by the former chief of OTS, Robert Wallace. And second, *The Moscow Rules*, authored by husband and wife team Jonna and Antonio Mendez, both of whom served in senior OTS positions (specifically 'chiefs of disguise'). For more details, see**:** Wallace, R. et al. *Spycraft*; Hoffman, D. E. *The billion dollar spy: a true story of Cold War espionage and betrayal,* [Kindle version] (London, Icon Books, 2017). Accessed 3 January 2018; Mendez, A. et al. *The Moscow rules*; Royden, B. G. 'Tolkachev, a worthy successor to Penkovsky', *Studies in Intelligence, CIA*, 47:3, 2008; Bury, J. 'Project Kalina: the Lotos operation conundrum', *Cryptologia*, 36:2, 2012; Weiser, B. *A secret life: the Polish officer, his covert mission, and the price he paid to save his country*, [Kindle version] (New York, Perseus, 2004). Accessed 1 February 2018; Macrakis, K. *Seduced by secrets*; Easter, D. 'Soviet Bloc and Western bugging of opponents' diplomatic premises during the early Cold War', *Intelligence and National Security,* 3:1, 2016; Gordievsky, O. *Next stop execution: the autobiography of Oleg Gordievsky,* [Kindle version] (London, Endeavour Media, 2018). Accessed 20 August 2020; MacIntyre, B. *The spy and the traitor; the greatest espionage story of the Cold War,* [Kindle version] (London, Penguin Books, 2019). Accessed 24 June 2019; Clarridge, D. R. *A spy for all seasons*; Crumpton, H. A. *The art of intelligence: lessons from a life in the CIA's clandestine service*, (New York, Penguin Books, 2012).

counterintelligence threats were low, the need for innovative tradecraft and technology was generally slim, as argued by one former SIS officer, "[all] those gadgets: that was just for Moscow hands".[53] And yet, not all agents who worked in Moscow offer substantial insights into technological tradecraft. For example, Soviet diplomat Aleksandr Ogorodnik, and GRU general Dimitri Polyakov, were both trained with sophisticated spy gear in preparation for their return to Moscow, but there is only a small amount of information about Ogorodnik's experiences once he returned to the capital (although there is good information about his use of subminiature cameras while posted in Bogotá), and the literature offers even less about Polyakov's experiences following his own return to Moscow (despite being lauded as the CIA's "jewel in the crown").[54] In some cases, agents who were posted to Moscow simply avoided espionage altogether. When SIS's prized agent, Oleg Gordievsky, returned from Copenhagen to Moscow, he was placed "on ice", meaning SIS made no attempt to communicate either impersonally or interpersonally to avoid taking unnecessary risks.[55]

Consequently, no case offers as much insight into innovative tradecraft as Adolf Tolkachev's. As a Soviet military engineer recruited in the late 1970s, Tolkachev is the only well-documented agent recruited and handled *entirely* within the confines of Moscow.[56] Secure tradecraft was paramount to sustaining his espionage in hostile conditions, but those same conditions mired the CIA's attempts to introduce technology into his operation. Given these unique circumstances, studies of his case, including lengthy accounts by Barry Royden and David Hoffman, explore in extensive detail the

[53] Grey, S. *The new spymasters: inside espionage from the Cold War to global terror,* (New York, Viking, 2015), p. 251.
[54] Mendez, A. et al. *The Moscow rules,* p. 48-58 & 171.
[55] Gioe, D. 'Handling HERO', p. 169.
[56] Royden, B. G. 'Tolkachev, a worthy successor to Penkovsky', p. 5-33; Hoffman, D. E. *The billion dollar spy,* see chapters 4-14.

challenges he and his handlers faced in adapting their tradecraft for Moscow rules.[57] Indeed, the conditions into which he spied were considered so incredible, that one former CIA officer, Benjamin Fischer, still believes that Tolkachev was more likely a KGB double agent - Fischer's claims have since been described as 'speculative' at best, but they underscore Tolkachev's uniqueness.[58] David Weiser offers similar insights in his study of Ryszard Kuklinski, a Polish general recruited abroad but eventually recalled to Poland.[59] Due to his restricted travel and length of stay in Warsaw, Kuklinski experienced a multitude of operational complications in the later stages of his operation.[60] As with Tolkachev, Kuklinski incorporated sophisticated tradecraft into his operation, but he was mired by constant counterintelligence threats, thus complicating its application.[61] To apply a selective case-studies approach would, therefore, lean heavily towards Tolkachev and Kuklinski at the expense of broader understanding. More to the point, it would exclude insights into tradecraft that was not applied in specific named cases, especially methods that were deemed useless or too dangerous in Moscow conditions, methods that could still reveal a great deal about the underlying causes of failure. Thus, rather than focus on individual cases, this analysis is structured around broader themes within the four tradecraft functions identified in the literature review (recruitment, surveillance, handling, and collection), but supplements these findings with named examples wherever possible.

[57] Ibid.
[58] Fischer, B. B. 'Fictitious spies and fake history', *International Journal of Intelligence and Counterintelligence*, 33:1, 2019, p. 170-175; CIA (29 March 2016) The billion dollar spy: a true story of Cold War espionage and betrayal, *reviewed by Nicholas Dujmovic.* Available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-60-no-1/the-billion-dollar-spy.html [accessed 12 January 2021].
[59] Weiser, B. *A secret life*, see chapters 1-12
[60] Ibid, see chapter 9.
[61] Ibid.

Recruitment

All espionage begins with recruitment, but finding and convincing someone to betray the state is a complicated task. While some agents were identified through surveillance (as discussed ahead), and some volunteered their services, others would need to be found by cultivating relationships and expanding social circles. The 'embassy cocktail circuit' was an oft-cited source of rapport building, and precisely how one SIS officer, named Bromhead, established an acquaintance with Gordievsky.[62] Yet even if someone of value could be found, few people were willing to betray the Soviet regime. Becoming a spy was no easy proposition for Soviet officials, who knew, all too well, the tremendous price they and their families could pay for the mere suspicion of betrayal.[63] Indeed, rumours abounded for years that famous spies including Popov and Penkovsky were burned alive in furnaces as lessons to would-be traitors.[64] Given these fears, asking the question, 'would you like to work for the CIA?' was never straightforward, as one former CIA officer attests:

> As you move into the recruitment "pitch" and the full dimensions of what you are asking dawns on the prospective agent, he or she looks at you with consummate disbelief, even when he or she more or less expects something is coming. Although perhaps not articulated, their eyes scream that what you want is the most ludicrous thing ever requested of them.[65]

In order to bring a source into an amenable mindset, they would need to be pulled into a relationship through the full force of the intelligence officer's 'personality and leadership.'[66] Emotional acuity was key, with feelings of greed, resentment, or revenge

[62] MacIntyre, B. *The spy and the traitor*, p. 47.
[63] Fischer, B. B. 'Fictitious spies and fake history', p. 171.
[64] CIA (21 January 2011) A look back … CIA asset Popov arrest. Available at: https://www.cia.gov/news-information/featured-story-archive/2011-featured-story-archive/pyotr-popov.html [accessed 14 August 2017]; Harding, L. (29 December 2018) 'Will they forgive me? No': ex-Soviet spy Viktor Suvorov speaks out, *The Guardian.* Available at: https://www.theguardian.com/world/2018/dec/29/ex-soviet-spy-viktor-suvorov [accessed 29 December 2018]
[65] Clarridge, D. R & Diehl, D. *A spy for all seasons*, p. 50.
[66] Ibid.

twisted by skilful manipulators into a common ground.[67] Emotions would 'bind' the recruiting officer and their target together, making recruitment possible.[68] But key to any successful pitch was knowing when the time was right to push, or when the time was right to give the recruitment target space to take stock of the reality unfolding around them.[69] As one former SIS officer noted, "[if] you push too hard, too quickly, it can go wrong … When it goes right, it is often because you don't push".[70] Throughout this process, the recruiter also had to assess their target's suitability for spy work, through questions and tasks that were designed to seem innocuous.[71] The former Soviet intelligence officer Viktor Suvorov, for instance, recalls how potential candidates were asked, through one excuse or another, to complete simple tasks, each slowly accustoming the target to clandestine work, '[maybe] he will be asked to accept at his address and forward to the officers letters ostensibly from his mistress, or to buy a complete set of telephone directories and give them to the officer as if he did not know how or this could be done. By degrees the tasks become more complicated, but the payment for them grows equally'.[72] Even if the information provided by the target was of meagre value, the act itself demonstrated the target's access to information, aptitude for spy work,, and their willingness to cooperate.

But this delicate relationship had to be developed in complete secrecy from Soviet security services, and without the target realising the intelligence officer's true intentions. If the KGB ever became aware, they would either put a swift end to the friendship or turn the intelligence officer's target into a 'dangle'.[73] Dangle's (also

[67] Crumpton, H. A. *The art of intelligence*, p. 60
[68] Ibid.
[69] Clarridge, D. R & Diehl, D. *A spy for all seasons*, p. 143
[70] MacIntyre, B. *The spy and the traitor*, p. 55.
[71] Suvorov, V. *Soviet military intelligence*. (London, Hamilton, 1984), p. 109.
[72] Ibid.
[73] Cherkashin, V. & *Feifer, G. Spy handler: memoir of a KGB officer*, (New York, BasicBooks, 2005), p. 104-106.

known as double agents, if they made it to handling) were seemingly legitimate sources who served as pawns for counterintelligence; for example, under KGB instruction, a Soviet official might play along with their newfound friend's advances, to learn more about their intentions. As the relationship developed, the dangle might be recruited as a full blown CIA agent, through which the KGB could feed deceptive intelligence all the way to American policymakers. Generally speaking sources with good access to information were never dangled, because creating a convincing ruse often required valuable intelligence, a price too high to pay if the dangle knew highly sensitive secrets.[74] Nonetheless, in the absence of any supportive evidence (such as data collected through surveillance), determining a target's loyalties took time and patience. It took, as a case in point, multiple meetings for Bromhead to trust Gordievsky, who was in part distrustful of the seeming ease of their relationship.[75] Eight months of no contact followed, which in part may have occurred because an overly distrustful Bromhead 'had applied the brakes harder than intended'.[76] It took a second meeting in a more seclusive hotel for Bromhead's trust in Gordievsky to evolve, a meeting that initially continued from a point of deep suspicion:

> …everything was still too easy. My suspicious mind was unable to accept this man at face value. My instinct was telling me that he was a remarkably nice person and I could trust him. My training and experience of KGB officers, on the other hand, was screaming caution.[77]

In the end, Bromhead decided to trust his gut and take a chance, nonetheless, his hesitancy underscores the interpersonal complexion at the heart of recruitment. There were two important factors in trusting Gordievsky.[78] First, the KGB rarely ever dangled one of their own officers, since they were in a position to compromise the Soviet's own

[74] Ibid.
[75] MacIntyre, B. *The spy and the traitor,* p. 52-56.
[76] Ibid.
[77] Ibid.
[78] Ibid.

intelligence operations, and second, Dutch surveillance had suggested that Gordievsky was disaffected with the Soviet regime.[79] Without those supporting factors, Bromhead held good reason to remain somewhat distrustful of an overly friendly KGB officer, who seemed suspiciously enthusiastic about wining and dining with his British counterpart.

Personal meetings thus offered the most socially engaging pathway for developing trust between the parties, but they were highly insecure. One simple technique was to formally invite an official to a social encounter, such as a dinner party or restaurant, yet Eastern Bloc officials were supposed to report formal invitations to their superior officers, potentially alerting security services to the relationship.[80] In some cases, principal agents with justified reason to travel abroad could meet Soviet officials on behalf of recruiting officers.[81] Greville Wynne, for example, was recruited by SIS due to his access to Eastern Bloc sources while working as an international salesman.[82] But such individuals had to be highly trusted, could only meet Soviet citizens within the confines of their profession, and like nonofficial cover operatives, they were not protected by diplomatic immunity.[83] Alternatively, operatives ran so-called "chance encounters", ostensibly accidental meetings often held on street corners,

[79] Ibid, p. 58-59; Fischer, B. B. 'Double troubles: the CIA and double agents during the Cold War', *International Journal of Intelligence and Counterintelligence*, 29:1, 2016, p. 54.
[80] Clarridge, D. R & Diehl, D. *A spy for all seasons*, p. 128.
[81] Copeland, M. *The real spy world*, (Weidenfeld & Nicolson, 1975), p. 110-112; CIA (14 February 2018) Romeo spies. Available at: https://www.cia.gov/news-information/featured-story-archive/2018-featured-story-archive/romeo-spies.html [accessed 20 July 2020]; Clarridge, D. R & Diehl, D. *A spy for all seasons*, p. 131-134.
[82] Duns, J. *Dead drop*, see chapter 2; Scott, L. 'Espionage and the cold war: Oleg Penkovsky and the Cuban missile crisis', *Intelligence and National Security*, 14:3, 1999, p. 25.
[83] Wynne, as a case in point, was arrested in Budapest for his involvement in the Penkovsky case, flown to Moscow, sentenced to eight years imprisonment, and served around a year in a Vladimir prison before being released in a spy-exchange. As he later reflected "I suppose that James Bond would have spat from his mouth a gas capsule (concealed in his molar) which would have overcome everyone but himself and would then have leapt to safety with a parachute concealed up his backside. But I regret to reveal that the British Intelligence Service lags behind Bond in ingenuity". However, as Corera notes, Wynne's harsh detainment led to 'much soul searching' in SIS about the use of principal agents. For more details, see Corera, G. *The art of betrayal*, p. 174-175.

in local shops, or even outside a target's place of work.[84] These seemingly coincidental encounters required no prior permission, but the recruiter required exact knowledge of the target's whereabouts and remained highly vulnerable to surveillance. Clarridge's accounts underscore these issues, as he describes relying on a Turkish friend and acquaintance to schedule chance encounters with a married couple of Polish consulate workers, dubbed Slava and Irina Adamski, whom he was trying to recruit in Turkey. He would wait outside his friends office, who worked with Slava, since it offered the perfect opportunity to catch him alone:

> Adamski emerged. As he put up his umbrella I walked by and virtually ran into him. It wasn't subtle but it worked. He was obviously surprised to see me, but he seemed pleased. We chatted beneath our umbrellas for a few minutes, and because it was near lunchtime, I invited him to a *lahmacun* restaurant to join me for the Turkish version of pizza. He hesitated, then accepted.[85]

In the early years of the Cold War, the East / West division of Berlin and Vienna offered an ideal opportunity for chance encounters. Prior to the Berlin Wall, Soviet and East German citizens who seamlessly travelled over the border to West Berlin (often to peruse pubs or visit the cinema) made for ideal targets, as chance meetings could be held in seemingly ordinary circumstances far away from the pervasive glare of the KGB.[86] If possible, operatives would even set up fake job adverts to lure potential candidates across the border, offering both a safe environment and a rationale to ask probing questions about their access to secrets.[87]

But many Soviet officials who travelled abroad were forced into groups and allocated KGB minders to ward off untoward contact with outsiders. Former KGB officer Victor Sheymov provides an account from one minder who knocked a Soviet

[84] Clarridge, D. R & Diehl, D. *A spy for all seasons*, p. 131-133.
[85] Ibid.
[86] Maddrell, P. *Spying on science: Western intelligence in divided Germany 1945-1961,* (Oxford, Oxford University Press, 2006), p. 122 – 129.
[87] Ibid.

scientist unconscious as he tried to defect to Swiss police in Geneva, "I said good-bye, wished him well, and hit him in the head as hard as I could with the only thing I had in my hand – my camera".[88] The scientist was then swiftly returned to Soviet territory, "[that] bastard's doing his fifteen year's hard labor".[89] Even if officials were not assigned oppressive minders, running safe chance encounters required a great deal of time and patience. Bromhead waited into the early hours of freezing cold mornings to approach Gordievsky while the latter played badminton, knowing it was the perfect opportunity for privacy.[90] And while Clarridge ran a handful of chance encounters with the Adamskis, several of his attempts failed.[91] Eventually, his persistence paid off, with routine chance encounters strengthening bonds between the parties while assuaging his fear that the Adamskis might be dangles.[92]

But beyond personal meetings, opportunities for social communication were limited to the telephone and postal mail. Of the two, the telephone was the most socially engaging option, but both were heavily surveilled in the Eastern Bloc, and especially inside the Soviet Union.[93] At minimum, telephones belonging to intelligence officers and foreign diplomats in Moscow were constantly monitored, 'all lines into the offices and apartments of foreigners were tapped and monitored around the clock by a virtual army of eavesdroppers.'[94] Intelligence officers could get around this problem by losing their surveillance tails and calling from payphones, but if they were 'spotted by the KGB using a public phone, it might be traced.'[95] All payphones in Moscow 'were

[88] Sheymov, V. *Tower or secrets: a real life spy thriller,* [Kindle version] (New York, Harper, 2012). Accessed 18 May 2020, p. 90.
[89] Ibid.
[90] MacIntyre, B. *The spy and the traitor,* p. 51.
[91] Clarridge, D. R & Diehl, D. *A spy for all seasons,* p. 127-143.
[92] Ibid.
[93] Macrakis, K. *Seduced by secrets*, p. 220.
[94] Mendez, A. J. & McConnell, M. *The master of disguise*, p. 221.
[95] Hoffman, D. E. *The billion dollar spy,* see chapter 4.

numbered', meaning the KGB 'could easily ask for an immediate trace' of any phone call made from a specific booth.[96]

Even if the operative called from a safe booth, they couldn't guarantee that their target's phones weren't also tapped. The KGB's intrusive tendencies stretched to the highest echelons of state, meaning the phones of senior ranking Soviet officials were routinely tapped.[97] The telephones of those close to Boris Yeltsin were all wiretapped due to his position as a potential challenger to Gorbachev's leadership.[98] It was also not unusual for maids and domestic staff to be recruited as KGB informants, or for listening devices (concealed microphones) to be placed in officials' premises.[99] To an extent some of these issues were reduced abroad, depending on the level of access the KGB could acquire over another country's telephonic infrastructure. For example, former CIA officer Richard Holm's describes how first contact with sources in Hong Kong often began by telephone, although the threat of Chinese technical eavesdropping was arguably slim in the then British controlled colony.[100] Similarly, Clarridge provided his personal phone number following his first encounter with the Adamskis, and later relied on the telephone to schedule personal meetings with Slava.[101] However, his decision carried dangers, since it was perfectly possible for Adamski to call from his home apartment or consulate, using phonelines that were almost certainly tapped and monitored by Polish security services.[102] Had they discovered that the Adamskis were scheduling unreported meetings with a mysterious American in a foreign country, it would have put an end to a recruitment opportunity.

[96] Ibid.
[97] I Mendez, A. J. & McConnell, M. *The master of disguise*, p. 221.
[98] Soldatov, A. & Borogan, I. *The red web*, see chapter 2.
[99] Copeland, M. *The real spy world*, p. 121-122.
[100] Holm, R. *The craft we chose: my life in the CIA*, (Oakland, Mountain Lake Press, 2011), p. 292-293.
[101] Clarridge, D. R & Diehl, D. *A spy for all seasons*, p. 130.
[102] Ibid.

Herein lay the issue of human behaviour, as owing to these dangers, recruiting officers required confidence in the sensibilities of the prospective spy. When inviting sources to a formal meeting or running chance encounters, the intelligence officer depended on that person to conceal the invitation from their respective security services.[103] Clarridge demonstrates this in his accounts, where he describes the difficult choice the Adamskis faced when he first invited them to dinner during their random encounter on a ferry:

> At this point he had a choice. He could report my invitation and seek clearance; if it was granted, this might mean that he was an intelligence officer, or it might mean that his consulate's intelligence personnel had decided to determine what I was up to and perhaps eventually allow me to "recruit" him so that they could run him as a double agent. I assumed the Polish intelligence service knew I was CIA, and if they had any doubt, the KGB could clear it up.
>
> Slava's other choice was to take a flier and come without checking, which is what I hoped—but doubted—he would do, because he would have been taking an enormous risk. The Adamskis would have to fabricate where they had gone that evening, since in their system you logged in and out twenty-four hours a day. If he was caught doing this, he could be sent home immediately and perhaps never assigned abroad again.[104]

And yet, if a formal invitation was accepted too willingly or seemed too easy, the recruiter had every reason to suspect that the target had formally reported the encounter. When Bromhead invited Gordievsky to dinner, the KGB officer's calm acceptance of the invitation, and suspicious choice of restaurant, only instilled further distrust in the SIS recruiter.[105] Gordievsky had requested to meet in a restaurant across from the Soviet embassy in Copenhagen, in a convenient spot for KGB surveillance, leading Bromhead to cable back to headquarters "[for] God's sake, I think *he's* trying to recruit me!" In fact, Gordievsky had strategically chosen the restaurant in order to *not* arouse KGB suspicions, falsely reporting the encounter to his superiors as an attempt to

[103] Ibid, p. 128.
[104] Ibid.
[105] MacIntyre, B. *The spy and the traitor*, p. 52-53.

recruit Bromhead, thereby gaining approval to meet. Only when Bromhead had developed at least some trust did he finally decide to invite his target to a confidential meeting, to which Gordievsky agreed.[106]

But similar problems applied to the telephone, since if a recruitment target decided to make a social call to the intelligence officer's apartment in Moscow, their relationship would likely have been immediately exposed. It was, for example, common practice for intelligence officers on both sides of the Iron Curtain to discourage their targets from making telephone calls to their homes or embassies.[107] However, almost all officials in the Eastern Bloc were wary of telephone tapping by their own government, leading to a sweeping sense of self-censorship personified by the Russian adage "this is not a phone conversation."[108] That was fortunate in one respect, because it reduced the likelihood that a Soviet official would carelessly call a recruiter's Moscow apartment. But it also meant that even if the intelligence officer safely called from a payphone, their target might be guarded about saying or sharing anything remotely sensitive over an insecure line. Clarridge demonstrated these issues in his accounts, noting how Slava Adamski made frequent calls to his apartment while in Ankara.[109] Since telling Slava to restrict his calls to a payphone risked revealing Clarridge's intelligence affiliations, he instead relied on a certain amount of hope that Slava would not be 'careless or naïve enough to call … from a phone monitored by his security personnel'.[110] When, however, Adamski did decide to call, he made it clear that he required Clarridge's help to organise an illicit abortion for his wife (Poland was 'staunchly Roman Catholic').[111] This factor helped to assure the CIA officer that not

[106] Ibid.
[107] Suvorov, V. *Inside Soviet military intelligence*, p. 109.
[108] Soldatov, A. & Borogan, I. *The red web*, see chapter 1.
[109] Clarridge, D. R & Diehl, D. *A spy for all seasons*, p. 139.
[110] Ibid.
[111] Ibid.

only was Adamski likely to have called from a secure phone booth, but he was also likely to have concealed their relationship or any further meetings from his superiors, since the abortion's discovery could have forced an unwanted return to Poland.[112] Only when the relationship between the two parties developed did Clarridge finally ask Slava whether he had been restricting their calls to public phones, to which 'Adamski didn't even deign to reply'.[113] Simply put, although phone calls could work, and despite the fact that many Soviets were aware of the risks, the intelligence officer still depended upon their source's common sense.

However, the uphill challenge of building a deep interpersonal relationship through high risk personal meetings or phone calls could be skipped altogether if agents volunteered their services. In many cases, volunteers would walk into embassies to pitch their services to foreign officials, but embassies were also under intense surveillance in many of the world's capital cities.[114] In fact, they were often considered so vulnerable, that anyone who made contact by walking into a major embassy was considered 'expandable', blown to counterintelligence from the moment they walked through the embassy gate.[115] Phoning embassies too was extremely dangerous, especially in countries where the security services could tap telephonic infrastructure.[116] Even in the United States, FBI phone tapping exposed several prospective American spies who unwisely telephoned the Soviet embassy in Washington.[117] In Moscow, the KGB tapped all US embassy lines and recruited Russian staffers who worked within the building.[118] KGB informers even worked 'inside the embassy itself as telephone

[112] Ibid.
[113] Ibid, p. 142.
[114] Copeland, M. *The real spy world*, p. 154-159
[115] Ibid.
[116] Wettering, F. L. 'Counterintelligence: the broken triad', in *Secret Intelligence: A Reader*, edited by Richrd J. Aldrich & Christopher Andrew (London, Routledge, 2009), p. 293.
[117] Ibid.
[118] Haseltine, E. *The spy in Moscow station: a counterspy's hunt for a deadly Cold War threat*, [Kindle version] (New York, Thomas Dunne Books, 2019). Accessed 10 May 2020, see chapter 1.

operators, where they could monitor who called and possibly even the calls themselves'.[119] As such, on counterintelligence home turf, a direct approach or call to an embassy was a gambit unlikely to succeed.

Outside of the volunteer's home territory, these risks were relatively mitigated. Sheymov decided not to pitch his request to defect at the US embassy in Moscow because of the extraordinarily high odds he'd be spotted by the KGB, instead choosing a slightly safer approach to the US embassy in Warsaw during a working trip.[120] In other key cases, Popov passed a letter into the car of an intelligence officer in Vienna, Kuklinski sent a letter to the US embassy in Bonn, and Polyakov simply approached FBI operatives while posted in New York.[121] Kuklinski's case even shows how telephoning embassies was acceptable tradecraft in countries where Eastern Bloc services were unable to tap embassy lines.[122] In his letter to the Bonn embassy, the Polish seaman specified that he would make contact again on two specific dates by phoning the US embassy's military attaché, requesting that whoever answered spoke either Polish or Russian. This, in part, was due to his limited free time, as he was expected to travel in groups of at least two, requiring a means to schedule impromptu meetings in brief moments of privacy.[123] But it underscores the point that in certain circumstances, the telephone was a useful tool for budding volunteers, on the condition that the volunteer called from an untapped line.

---

[119] Absher, K. M. et al. *Privileged and confidential: the secret history of the president's intelligence advisory board* (Lexington, University Press of Kentucky, 2012), p. 248.
[120] Sheymov, V. *Tower or secrets*, p. 288 & 349.
[121] West, N. *Historical dictionary of Cold War counterintelligence*, (Plymouth, The Scarecrow Press, 2007), p. 187; Grimes, S & Vertefeuille, J. *Circle of treason: a CIA account of traitor Aldrich Ames and the men he betrayed*, [Kindle version] (Annapolis, Naval Institute Press, 2012). Accessed 11 May 2020, see chapter 4; Trahair, R. C. S *Encyclopedia of Cold War espionage*, (Westport, Greenwood Publishing Group, 2004), p. 273.
[122] Weiser, B. *A secret life*, see chapter 1.
[123] Ibid.

For volunteers inside Moscow, however, there were few safe options. Penkovsky, who was one of a handful of successful cases, first approached two American students (named Cox and Cobb) on Moskvoretsky bridge, asking for a parcel to be delivered to the US embassy.[124] Despite their concerns, the students agreed to help, delivering his parcel containing valuable intelligence into the embassy's hands.[125] Upon hearing no response, he continued approaching foreign officials with whom he had a permitted working relationship, including the scientist Arthur Merriman and the salesman (and SIS liaison officer) Greville Wynne.[126] Tolkachev, by comparison, had no justifiable reason to interact with foreign officials, instead approaching cars with American license plates in gas stations, hoping to make contact with American diplomats.[127] His approach was extremely risky, because diplomats were expected to use reserved gas stations, which were considered surveillance "hot spots".[128] The KGB even deployed 'decoy cars', with fake diplomatic license plates, to entrap would-be volunteers using Tolkachev's technique.[129] And while the telephone was not a safe means of making direct contact, both Penkovsky and Tolkachev offered their phone numbers so that intelligence officers could respond, which was a dangerous move if the operative called from an insecure landline.[130]

Once again, the operational hazards placed greater emphasis on human behaviour, as successful pitches in Moscow required mounting trust in the person pitching their services. Anyone who walked into a heavily surveilled embassy was considered 'expendable' from the moment they set through the door, while those who

[124] Corera, G. *The art of betrayal,* p. 135; Duns, J. *Dead drop,* see chapter 2.
[125] Ibid.
[126] Ashley, C. *CIA spymaster,* p, 150 – 151; Duns, J. *Dead drop,* see chapter 2.
[127] Royden, B. G. 'Tolkachev, a worthy successor to Penkovsky', p. 6.
[128] Fischer, B. B. 'Fictitious spies and fake history', p. 169.
[129] Fischer, B. B. 'The man who wasn't there', *International Journal of Intelligence and Counterintelligence,* 30:1, 2017, p. 32.
[130] Duns, J. *Dead drop,* see chapter 2; Royden, B. G. 'Tolkachev, a worthy successor to Penkovsky', p. 8.

tried to call by telephone were just as likely to be ignored. Frederick Wettering, for instance, described the Americans who phoned the Soviet embassy in Washington as 'low-level (and dumb), would-be spies'[131] But even if the volunteer made a secure approach, the onus was on them to prove that they were not a KGB provocation sent to entrap foreign officials.[132] Outside of Moscow, intelligence officers were often more willing to meet volunteers on face value, but in Soviet territory a provocation could mean the arrest and exile of an undercover operative.[133] Indeed, despite the fact that Kuklinski was considered a low ranking seaman when he first volunteered, he was nonetheless given a fair hearing.[134] But in Soviet territory, clear evidence of a person's sincerity and access to valuable information was required, material that could quickly incriminate the volunteer if it ever found its way into KGB hands.[135] This was exemplified in the case of Aleksandry Cherepanov, who used an American liaison to deliver secret papers to the US embassy in Moscow.[136] Despite protests from intelligence officers, the overreactive diplomatic official who received his papers decided that the threat of a Russian provocation was too great, returning Cherepanov's documents to the Soviet Foreign Ministry.[137] And since his name was included in his package, he was immediately tracked down and executed.[138] In this case, the volunteer made the decision to provide proof of his credibility through hard intelligence, and as such he was condemned to death. And while it was common for embassies to turn away

[131] Wettering, F. L. 'Counterintelligence', p. 293.
[132] Copeland, M. *The real spy world*, p. 154-159.
[133] Weiser, B. *A secret life*, see chapter 1.
[134] Ibid.
[135] Hoffman, D. E. *The billion dollar spy*, see chapter 3.
[136] Bagley, T. H. *Spy wars: moles, mysteries, and deadly games*. [Kindle version] (New Haven, Yale University Press, 2007). Accessed 1 February 2018, see chapter 16.
[137] Ibid.
[138] Sager, J. *Uncovered: my half-century with the CIA*, (Bloomington, WestBow Press, 2013), p. 152-154.

volunteers, it was not common for US officials to write 'the death sentence for the man making the offer'.[139]

Other agents too were prepared to take the chance. Sheymov as a case in point was quickly taken seriously, despite his high risk embassy approach, because he immediately proved himself to be a KGB cipher clerk; cipher clerks had access to encryption keys, and were considered to be extremely valuable.[140] Penkovsky, too, was prepared to take the chance, providing clear samples of his intelligence in his first package to the US embassy.[141] Unfortunately, the CIA's Moscow cohort had been gutted in the wake of the Popov operation around a year earlier, leaving it without any means to securely respond.[142] Their only man on the ground was an inexperienced officer codenamed COMPASS, who fumbled in every attempt to make contact.[143] When he tried to call the number given by Penkovsky, he 'rang the number an hour after the scheduled time and spoke in such garbled Russian that Penkovsky hung up, mystified'.[144] These failings were unknown to Penkovsky, who continued pitching his services to foreign nationals in the hope that someone might respond.[145] As reports of his frequent unanswered pitches reached CIA officers, who were still unable to respond, one remarked that Penkovsky would probably "hang himself" soon enough, adding "[how] many strikes does one have before he's out in a baseball game?"[146] In the end, he succeeded through Wynne, but his success was heavily owed to his own willingness to offer bona fides, and his determination to keep making dangerous pitches until someone from the other side finally replied.

[139] Ibid.
[140] Sheymov, V. *Tower or secrets,* p. 349 – 350.
[141] Ashley, C. *CIA spymaster,* p, 146.
[142] Ibid.
[143] Duns, J. *Dead drop,* see chapter 2.
[144] Ibid.
[145] Ashley, C. *CIA spymaster,* p, 150 – 151.
[146] Ibid, p. 151.

By contrast, Tolkachev, who was well aware that his gas station approaches were dangerous, painstakingly tried to avoid sharing personally identifiable information, especially raw intelligence, leading the CIA to constantly rebuff his efforts.[147] One of the cars he frequently approached was (unknown to him) driven by the CIA's Station Chief, who despite knowing the likelihood of a KGB provocation, was impressed by Tolkachev's tenacity. But on each occasion Tolkachev offered no convincing bona fides, offering only snippets of information about his *potential* access along with instructions to arrange a meeting.[148] Langley, still reeling from the paranoic Angleton era, was unprepared to take the chance, concluding that unless Tolkachev proved his value, he was too dangerous:

> We have no proof that [Tolkachev] is a provocation, but his approach to us has many of the earmarks of previous cases that we found to be under KGB control. Even if he was bona fide in the beginning, his several attempts to contact us could have brought him under discreet coverage by the KGB. At best, we view [Tolkachev's] bona fides and potential as unproven—in contrast to existing sources in Moscow whom we have not been able to contact during the operational standdown.[149]

Consequently, on several occasions the station chief was forced to ignore Tolkachev, even as he stood outside the vehicle. The situation became increasingly clear to the scientist, who's enthusiasm to take chances was quickly waning: "I'm afraid for security reasons to put down on paper much about myself, and, without this information, for security reasons you are afraid to contact me, fearing a provocation".[150] Even when he finally decided to provide his phone number, as a 'secure way to pass key identifying data on himself', he refused to take any chances, providing 'all but two of the digits in his phone number', with the remaining digits written on pieces of

[147] Hoffman, D. E. *The billion dollar spy*, see chapter 2.
[148] Ibid.
[149] Ibid, see chapter 3.
[150] Royden, B. G. 'Tolkachev, a worthy successor to Penkovsky', p. 8.

plywood that he would hold at a specific time and date.[151] Moscow Station's decision to contact Tolkachev by this tentatively secure system was emboldened when he passed yet another envelope into an American car, containing eleven pages of handwritten materials, including his identity, address, workplace, position, and impressive detail on Soviet military technologies.[152] Nonetheless, without this hard evidence, which Tolkachev knew to be extremely risky, Moscow Station would have had good reason to continue ignoring a highly valuable volunteer. As such, although it was perfectly possible for a Soviet official in Moscow to volunteer safely, the success of the methods they used hinged on their own common sense, awareness of the dangers, and their willingness to provide crucial evidence.

Surveillance

One way to reduce the burdens in recruitment was to find alternative sources of 'operational data', meaning information that aids in the spotting and assessment of sources.[153] In fact, with enough prior assessment information, recruiters could successfully deliver so-called 'five-minute' pitches (sometimes known as cold pitches), in situations where there was little opportunity for cultivation.[154] Herein, aside from receiving snippets of information from sources (such as classified phonebooks), surveillance offered a window into a target's private affairs. Any intelligence officer 'worth his salt' would run routine street surveillance of their targets, to observe how they lived 'outside of working hours.'[155] During the Adamskis recruitment, for example, Clarridge kept the couple under close observation using teams of clandestine

[151] Ibid.
[152] Hoffman, D. E. *The billion dollar spy*, see chapter 4.
[153] Copeland, M. *The real spy world*, p. 116-118.
[154] Wallace, R. et al. *Spycraft*, p. 364.
[155] Ibid, p. 118.

CIA officers to monitor their movements after each meeting, who in turn reported nothing suspicious.[156] But the ideal goal was to spot something that might be turned into a weakness, as exemplified when Dutch surveillance teams thought they'd spotted Gordievsky buying homosexual pornography.[157] Subsequent efforts to send a male honeytrap in Gordievsky's direction eventually proved fruitless, because 'Gordievsky was not gay. He had not realized he was being chatted up'.[158] Nonetheless, the attempt emphasises the point that the most effective surveillance provided evidence of a target's indiscretions to leverage for recruitment. Nothing, in this sense, was out of bounds, Copeland even describes how the CIA maintained a high-end French brothel for recruitment purposes:

> In the early days of the CIA, the espionage branch for a while helped the French SDECE maintain a high-grade brothel in Paris for the purpose of luring diplomats into compromising positions. It turned out, however, that the main customers were Middle Easterners, Americans, and Australians (in that order), with no Bloc diplomats at all, so the participation fizzled out – just at the time, incidentally, when the house was beginning to make huge profits.
>
> The CIA is now out of the brothel business. All the same, the CIA, the SIS, the KGB, and other modern intelligence services … keep a close eye on brothels, call girl agencies, massage parlors, shady nightclubs, and even mailing lists for pornographic literature and respondents to set advertisements, in the hope of spotting the name of a person on whom they would like to have blackmail information, or on whom they would not want the opposition to have blackmail information.[159]

'Audio surveillance', meaning the 'bugging' of a target's premises or workplace with hidden microphones and phone taps that transmitted data to nearby listening posts, was often far more efficient.[160] One of the most famous examples of bugging was a Soviet device dubbed "The Thing". For seven years, it was concealed in a replica of the Great Seal of the United States, gifted to a US ambassador in 1945, and hung above his office

[156] Clarridge, D. R & Diehl, D. *A spy for all seasons*, p. 146.
[157] Macintyre, B. *The spy and the traitor*, p. 29.
[158] Ibid, p. 35.
[159] Copeland, M. *The real spy world*, p. 153-154
[160] Dulles, A. W. *The craft of intelligence*, p. 63.

in Moscow.[161] As Kennedy notes, '[the] ambassador hung the seal in his office at his Spasso House residence in Moscow', where it 'presumably yielded a wealth of classified information to Soviet listeners until its discovery in 1952.'[162] For its time, the device was deemed a technologic marvel, forwarded to MI5 scientist, Peter Wright, to determine its mechanism and construct a replica.[163] But scientific advances soon led to further reductions in the size of listening devices and increased the longevity of battery life, vastly expanding the potential of eavesdropping operations.[164] In turn, audio plants became a key mission for both sides of the Iron Curtain, most often by bugging embassies and consulates before new tenants arrived.[165] The Soviets became so troubled by this risk that they began refusing 'to permit local service people to install telephones or even ordinary electrical wiring in the buildings they occupy'.[166] Placing a bug in a building that was occupied, however, was a complicated endeavour, as Marchetti & Marks explain:

> A classic, highly dangerous operation calls for a great deal of planning during which the site is surveyed in extensive detail. Building and floor plans must be acquired or developed from visual surveillance. The texture of the walls, the colors of the interior paints, and the like must be determined. Activity in the building and in the room or office where the device is to be installed must be observed and recorded to ascertain when the area is accessible. The movements of the occupants and any security patrols must be also known. When all this has been accomplished, the decision is made as to where and when to plant the bug.
>
> Usually the site is entered at night or on a weekend and, in accordance with carefully pre-planned and tightly timed actions, the audio device will be installed. High-speed, silent drills may be used to cut into the wall and, after installation of the bug, the damage will be repaired with quick-drying plaster and covered by a paint exactly matching the original. The installation may also be accomplished from an adjoining room, or one above or below (if a ceiling or

[161] Ibid.
[162] Kennedy, R. *Of knowledge and power: the complexities of national intelligence,* (Westport, Praeger Security International, 2008), p. 40.
[163] Wright, P. & Greenglass, P. *Spycatcher*, p. 20-26.
[164] Albeit, such imagination occasionally exceeded reality, including rejected proposals by intelligence officers to install microphones by dangling out of helicopters, "A helicopter hovering in central Madrid with a case officer dangling from a rope ladder would likely be noticed". For more details, see Wallace, R. et al. *Spycraft*, p. 171.
[165] Easter, D. 'Soviet Bloc and Western bugging of opponents', p. 28-46.
[166] Dulles, A. W. *The craft of intelligence,* p. 64.

floor placement is called for).[167]

Wright, who claims to have 'bugged and burgled' his way across London, described one operation to bug a Soviet consulate in Bayswater Road, which entailed many of the complications above.[168] The operation involved drilling into a partitioning wall between the Soviet consulate on one side, and an empty building on the other, producing a tiny pinhole that was 'almost invisible to the naked eye'.[169] The microphone would transmit information 'out into the street and back along telephone wires to Leconfield House, where amplifiers boosted the captured sound into intelligible speech'.[170] Unfortunately for his team, the embassy's tenants, by either intent or unlucky coincidence, painted over the pinhole, leading to a new operation that required 'considerable planning', including the mounting of fourteen foot scaffolding, observation posts, radios, and plaster and paints to repair incriminating damage.[171]

Even smaller operations, such as those mounted against the apartments of diplomatic officials or hotel rooms, carried considerable risks.[172] Crumpton recounts one illicit entry which required both an intelligence officer and a technical specialist in the same dangerous space (one to handle operational issues and the other to manage the equipment). This delicate operation entailed a range of unpredictable factors, including a patrolling policeman who was quickly pacified by a look-out (stationed outside) using friendly chit-chat and free alcohol. Crumpton was also surprised to discover the occupant's cat, but had that cat been a dog (one with a bark loud enough to rouse the neighbours) the entire operation could have been exposed. The point being, breaking

[167] Marchetti, V. & Marks, J. D. *The CIA and the cult of intelligence,* (London, Jonathan Cape, 1974), p. 188 - 189
[168] Wright, P. & Greenglass, P. *Spycatcher,* p. 54 – 59.
[169] Ibid, p. 59.
[170] Ibid.
[171] Ibid, p. 59 – 60.
[172] Crumpton, H. A. *The art of intelligence,* p. 67-71.

and entering into a private apartment was a risky act, and often required prior knowledge of the premises and its potential hazards.[173] Even if listening devices were safely planted, there was every possibility that technical 'sweeping' (using sophisticated equipment to detect hidden microphones) would eventually unearth the bug.[174] In 1964, for example, audio sweepers (armed with new equipment) detected bugs in almost every room of the US embassy in Moscow.[175] And when the KGB developed a highly advanced sweeping device in the 1970s, they found around two dozen bugs in one Asian embassy alone, some 'more than twenty years old with corroded batteries.'[176] In Wright's case, the Soviets detected the pinhole for a second time, filling the intruding hole with cement.[177] But this may have been owed to the KGB's habit for entirely redecorating rented buildings in foreign countries (putting in new walls, floors and ceilings over the original foundations), 'baffling the effectiveness of any bugs that may have been installed.'[178]

Wright also notes how 'an occasional decorator and odd-job man for the Russians', codename Nutkin, played a key role in the Bayswater Road operation, by supplying important information about the partitioning wall's measurements.[179] Without that agent, MI5 would not have been able to drill the hole to appear directly behind a concealing cornicework, nor would they have known that the Soviets had 'completely remodeled' the room with a 'soundproofed partition'[180] It was actually not unusual for technical surveillance operations to depend upon an insider source, as

[173] Ibid.
[174] Wallace, R. et al. *Spycraft,* p. 192-193.
[175] Aldrich, R. J. *GCHQ: the uncensored story of Britain's most secret intelligence agency* [Kindle version] (London, HarperPress, 2010). Accessed 1 February 2017, p. 179.
[176] Wallace, R. et al. *Spycraft,* p. 230
[177] Wright, P. & Greenglass, P. Spycatcher, p. 60-61.
[178] Marchetti, V. & Marks, J. D. *The CIA and the cult of intelligence,* p. 190.
[179] Wright, P. & Greenglass, P. Spycatcher, p. 59.
[180] Ibid, p. 61.

Dulles argues, 'the trick is to find the man who can do the job and who has the talent and the motive, whether patriotic or pecuniary':

> There was on instance when the Soviets managed to place microphones in the flowerpots that decorated the offices of a Western embassy in a neutral country. The janitor of the building, who had a weakness for alcohol, was glad to comply for a little pocket money. He never knew who the people were who borrowed the pots from him every now and then or what they did with them.[181]

That was relatively easy for Wright's team, since Nutkin was a British citizen who was easy to access and likely to cooperate, but outside of friendly territory the odds were less favourable.[182] With the exception of cases such as the one described by Dulles, intelligence officers would logically need to find a cooperative worker willing to surreptitiously bug one of the most guarded buildings outside of the Soviet Union. Such factors, combined with other operational hazards, largely restricted the feasibility of audio operations in occupied embassies.[183]

The limitations of microphone and battery technology were also restrictive factors, since it was not uncommon for bugs to corrode or stop working, thus putting an end to an otherwise effective operation.[184] Moreover, even when listening devices functioned as expected, their results would often be rendered useless by noisy interference.[185] Listening devices picked up all sounds in their vicinity, meaning important conversations were left inaudible by background noise: '[a] bug placed in the couch of a Chinese diplomat in France proved ineffective because of the squeaking noises that drowned out conversations, not only when the diplomat was using it for his frequent sexual escapades but when visitors were simply sitting.'[186] CIA engineers even

[181] Dulles, A. W. *The craft of intelligence,* p. 64
[182] Wright, P. & Greenglass, P. *Spycatcher,* p. 59.
[183] Easter, D. 'Soviet Bloc and Western bugging of opponents', p. 29.
[184] Ibid, p. 42.
[185] Richelson, J. T. *Wizards of Langley: inside the CIA's Directorate of Science and Technology*, [Kindle version] (Oxford, Westview Press, 2002). Accessed 1 March 2002, p. 146-147.
[186] Ibid.

tried to resolve this problem by surgically grafting a living cat with listening equipment, in an operation dubbed Acoustic Kitty.[187] The Frankenstein-esque experiment offered great promise, with the cat's cochlea, akin to a human ear, filtering out useless noise.[188] However, the operation ended when a failed test terminated any hopes for the project's future, as Richelson explains:

> … they slit the cat open, put batteries in him, wired him up. The tail was used as an antenna. They made a monstrosity. They tested him and tested him. They found he would walk off the job when he got hungry, so they put another wire in to override that. Finally, they're ready. They took it out to a park bench and said "Listen to those two guys. Don't listen to anything else—not the birds, no cat or dog—just those two guys!" … They put him out of the van, and a taxi comes and runs him over. There they were, sitting in the van with all those dials, and the cat was dead![189]

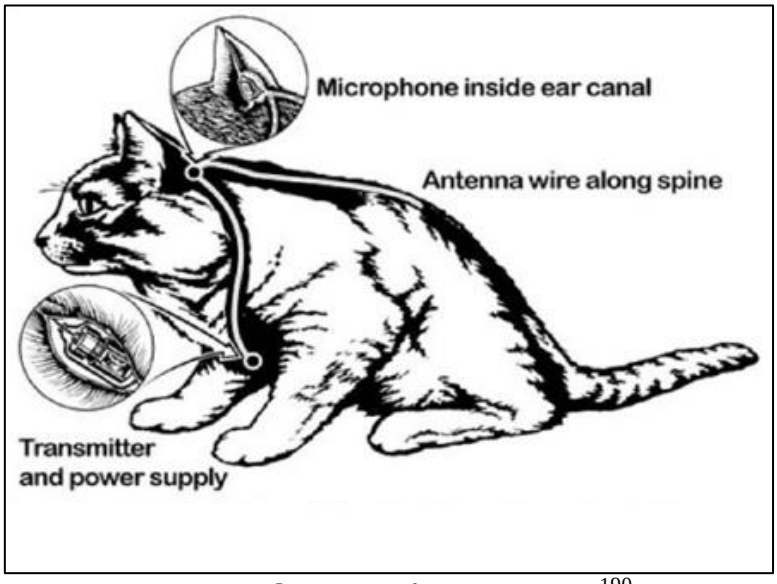

Figure 2: Operation Acoustic Kitty.[190]

Given these issues, audio operations were rarely ever undertaken in denied areas such as the Soviet Union, China or North Korea.[191] Instead, they were reserved for 'third world' countries or European capitals, where surveillance threats were reduced.[192] Yet, the CIA still recognised that each audio operation was an opportunity for useful results,

[187] Wallace, R. et al. *Spycraft,* p. 200-201.
[188] Richelson, J. T. *Wizards of Langley*, p. 146-147.
[189] Ibid.
[190] Wallace, R. et al. *Spycraft,* p. 202.
[191] Ibid, p. 159; Marchetti, V. & Marks, J. D. *The CIA and the cult of intelligence*, p. 189.
[192] Wallace, R. et al. *Spycraft,* p. 159.

and recruited an army of technicians across the globe ready to exploit any opportunity that arose.[193] Towards the later years of the Cold War, technological advances opened up the opportunity for so-called "quick plant" operations, which even became possible inside the USSR itself.[194] At one point operatives were able to bug a Moscow police shelter used by a variety of security services, including KGB surveillance teams.[195] However, because of the speed at which these operations had to take place, quick plant operations relied on a 'single bug with no redundancy and left no margin for installation complications or errors.'[196] That being said, one CIA officer, dubbed by Mendez as "Bull Monahan", built something of a reputation for his unique talents with lock picking and quick plant bugging operations.[197] 'Bull' was considered an expert in running 'audacious' operations against 'Communist targets … such as the hotel rooms and offices of Soviet bloc diplomats'.[198] It is, however, worth noting that the operative allegedly remained mindful of the potential pitfalls afflicting quick plant operations: 'Bull's fascination with the "gee-whiz" aspects of espionage technology did not blind him to the complexities of what he called the "operational stage"': all of the elements impinging on the problem at hand, such as locale, level of surveillance, and people involved'.[199] In other words, technology opened the doors to make these daring operations possible, but inside the Soviet Union they were still inordinately dangerous, performed only with a substantial amount of planning.

These risks had to be weighed against the odds of the target sharing anything of value, placing further emphasis on the need for trust. Embassies made for rich targets,

[193] Ibid.
[194] Ibid, p. 228-229.
[195] Ibid, p. 501-502.
[196] Ibid, p. 502.
[197] Mendez, A. J. & McConnell, M. *The master of disguise*, p. 183.
[198] Ibid.
[199] Ibid.

because although sensitive discussions were often held in soundproofed bubble rooms (which were encased inside the building itself to negate any microphones buried in the walls), they carried a wide eavesdropping net.[200] As Easter argues, they offered access to an array of recruitment targets, revealing 'potential weaknesses, exposing unhappy marriages, homosexual inclinations, money problems or doubts about their own government.'[201] Telephone tapping of the Soviet embassy in Bogotá, for example, revealed that Ogorodnik was having an affair with an unidentified woman.[202] This allowed one CIA officer to make a 'cold pitch' through a chance encounter in a sauna, offering Ogorodnik money and the opportunity to relocate to the West with his new mistress.[203] Gordievsky, who knew his embassy was likely bugged by Dutch intelligence, also telephoned his wife from his embassy in Copenhagen to complain about the Soviet invasion of Czechoslovakia, sending his "first, deliberate signal to the West".[204]

But while it was often easier to target specific individuals in their home or hotels, this naturally restricted the potential number of targets, as candidly put by one former diplomat: 'very few people would talk to their wives about sensitive political or military information. The value of the listening devices is to get somebody'.[205] Professional intelligence officers often made for difficult targets, because they knew how to spot the signs of a surreptitious entry. Gordievsky's apartment was bugged by Dutch Intelligence while he and his wife attended dinner with a local friend, but the

[200] As Easter notes, these 'normally consisted of large, soundproof, transparent plastic and aluminium boxes set up on stilts or suspended from the ceiling of empty rooms. A sound machine sometimes acted as a further barrier to eavesdropping inside the bubble – the British embassy in Moscow had the noise of a cocktail party playing continuously'. For more details, see Easter, D. 'Soviet Bloc and Western bugging of opponents', p. 31 & 41.
[201] Ibid.
[202] Fischer, B. B. 'Fictitious spies and fake history', p. 162.
[203] Ibid.
[204] Gordievsky, O. *Next stop execution*, see chapter 7.
[205] Easter, D. 'Soviet Bloc and Western bugging of opponents', p. 37.

trained officer placed a blob of glue between his front door and hinge before setting out to dinner, and after returning to find the seal broken he realised that his apartment had been entered and likely bugged.[206] CIA officer, Richard Holm, recounts a similar story, where he was encouraged by a Soviet diplomat (whom Holm's was trying to recruit) to purchase a piano for his daughter.[207] The piano salesman strangely knew Holm's name in advanced, leading Holm's and his wife to suspect that the piano had been pre-emptively bugged by the KGB. As a consequence, they stored the piano in the farthest corner of their apartment, avoided indiscreet conversation, and even hired a team of OTS technicians to quietly check the Reichenbach's innards for hidden microphones (who found nothing in the process).[208]

The fact that trained intelligence officers were wary of eavesdropping while working abroad is hardly surprising, however this tendency towards self-censorship extended to non-intelligence officials on both sides of the Cold War. As Aldrich argues, the spectre of '[secret] listening terrified friend and foe alike.'[209] In fact, Soviet citizens were often more worried about eavesdropping by their own security services than by foreign intelligence agencies. Copeland, for example, describes one incident where a Soviet official was overheard (ironically captured by a hidden CIA microphone) being chided by his wife 'for something indiscreet he had apparently said in the presence of a servant who had just left the room'.[210] After the worried diplomat asked his wife "[do] you suppose she is an American spy", she responded "God help us, let us *hope* so".[211] Moreover, Aldrich notes that during a visit by the British Prime Minister Harold Macmillan, Soviet premier Khrushchev and his inner circle grew frustrated about

[206] Gordievsky, O. *Next stop execution,* see chapter 7.
[207] Holm, R. *The craft we chose,* p. 344-347.
[208] Ibid.
[209] Aldrich, R. J. *GCHQ*, p. 53-54.
[210] Copeland, M. *The real spy world*, p. 122.
[211] Ibid.

eavesdropping by their own KGB, 'to the extent that they dared not speak freely, even amongst themselves in their own capital.'[212] Similarly, in 1966, President Tito of Yugoslavia discovered that he had been bugged by his own security chief, complaining to a friend that he'd found hidden microphones "everywhere … Even my bedroom!"[213] Yet, while officials were more than likely to refrain from scandalous behaviour, the subtlest indiscretions could still proffer value. Despite Gordievsky's best efforts to say nothing important in his expectedly bugged apartment, he could not conceal his marriage problems from Dutch eavesdroppers.[214]

Consequently, very few cases against Soviet officials returned meaningful results. As one CIA officer argued, "fifty percent of the audio operations were terminated every year, and probably half of those shouldn't have gone forward in the first place". [215] Due either to the target's discretion, or to the time taken to analyse, translate and transcribe days, weeks or even months' worth of recordings, only around five percent of operations produced ninety-five percent of useful data, an estimate that was considered optimistic.[216] But the chance that an operation would return nothing meaningful couldn't be taken for granted, especially if that operation entailed extraordinarily high risks. As Crumpton concluded after his six month bugging operation achieved zero results, in future missions he would first try to better understand his target's nature.[217] He would study his target's 'propensity for gab' and consult with the CIA's expert psychological assessments, adding that it 'was dumb to take risks without better understanding the odds of success.'[218] The point being, while it

[212] Aldrich, R. J. *GCHQ,* p. 4.
[213] Ibid.
[214] Macintyre, B. *The spy and the traitor,* p. 38.
[215] Wallace, R. et al. *Spycraft,* p. 231.
[216] Ibid.
[217] Crumpton, H. A. *The art of intelligence,* p. 70.
[218] Ibid.

was perfectly possible to run audio operations, even inside Moscow, the success of these cases depended on the target's behaviour, which was almost always skewed towards reservation rather than indiscretion.

Handling

Once either the source or the intelligence agency had taken a decision to cooperate, the two parties would move towards agent handling. By this stage, some degree of trust had developed between the parties, but the fact that even loyal spies could be turned at any point throughout their espionage career ensured that trust remained high on the agenda.[219] Popov, as a case in point, who was a deeply ideologically motivated agent, was forced to feed 'lousy information' to his CIA handlers after being discovered by the KGB.[220] With that in mind, akin to the bona fides provided by walk-ins, the most effective way to determine an agent's loyalty was through the constant production of high-quality intelligence (information that the opposing side would not willingly reveal).[221] But even highly productive sources could still be distrusted by ardent sceptics, with Penkovsky's production drawing doubts not for its sloppiness, but for the excellent quality of his photography, leading some in the CIA to ponder whether KGB stooges had taken the photographs on his behalf.[222]

It was thus necessary to develop interpersonal trust between the parties, but this was almost always a delicate process. Gordievsky found his first handler (dubbed Hawkins) to be cold and abrasive, a polar opposite to the affable SIS officer responsible

[219] As Scott illustrates, the doubts about Penkovsky's loyalties existed throughout and after his career. SIS chief, Sir Dick White, 'believed Penkovsky might have been turned by the spring of 1962'. For more details, see Scott, L. 'Oleg Penkovsky, British Intelligence, and the Cuban Missile Crisis', in *Learning from the secret past: cases in British intelligence history,* edited by Robert Dover and Michael S. Goodman, (Washington, Georgetown University Press, 2011), p. 250
[220] Ashley, C. *CIA spymaster,* p. 132-133.
[221] Wallace, R. et al. *Spycraft,* p. 366.
[222] Duns, J. *Dead drop,* see chapter 6.

for his recruitment (Bromhead was fittingly described by Gordievsky as having a tendency for turning up to 'embassy parties whether he had been invited or not').[223] Following a barrage of direct questions in his first encounter with Hawkins, Gordievsky recalled that he "did not like" the nature of his reception, having expected to be welcomed by SIS, not interrogated.[224] But as tensions between the two men eased throughout further meetings, their relationship grew more respectful, and in turn, more productive.[225] On the other hand, when Penkovsky's joint SIS and CIA handlers tried to assess their new agent, their differing operational philosophies created complications. The CIA, as part of its "asset validation" process, would test its agents with the polygraph machine, commonly known as the lie-detector test.[226] Indeed, Clarridge told Slava Adamski early in their relationship that it was routine practice for CIA officers and agents to be polygraphed, receiving no complaint.[227] SIS, however, rejected the CIA's request to polygraph Penkovsky, fearing it might humiliate their emotionally sensitive agent.[228] Instead, to settle concerns about his suspiciously high quality photography, they asked Penkovsky to photograph a series of magazines, a task through which he immediately proved his photographic skills.[229]

Ironically, as Gioe argues, the decision to avoid polygraphing Penkovsky may have been a misjudgement on SIS's part because their agent desperately wanted to be believed.[230] Penkovsky wanted to know that his intelligence would be valued by the

[223] Gordievsky, O. *Next stop execution*, see chapter 9.
[224] He specifically stated 'I was surprised, and not a little put out, to find the big man acting in a hostile, almost threatening manner. I expected our co-operation to begin in a spirit of friendliness and enthusiasm: I had hoped that the British would be grateful that I was offering help, and risking a good deal on their behalf. Far from it: Michael [the handler] lit off into a barrage of abrupt questions — 'Who is your Resident? How many KGB officers are there in the station?' — as gruffly if he were interrogating a prisoner'. For more details, see Ibid.
[225] Ibid.
[226] Gioe, D. 'Handling HERO', p. 151-152.
[227] Clarridge, D. R & Diehl, D. *A spy for all seasons*, p. 145.
[228] Gioe, D. 'Handling HERO', p. 151-152.
[229] Duns, J. *Dead drop*, see chapter 6.
[230] Gioe, D. 'Handling HERO', p. 151-153.

people it was intended for: "[perhaps] somebody who does not know me, who cannot look into my eyes like you, will say, 'Perhaps he copies all this about rockets of Pravda', or something like that."[231] Handling was always an interpersonal judgement that fluctuated with the personality of the agent - some might have taken offence to the polygraph while others would have felt vindicated. Similar issues arose when agents needed to be tasked or even instructed to reign in their production.[232] Sometimes spies needed to be discouraged from taking unnecessarily dangerous risks, '[it] is a timeless adage in intelligence services that if you do not have control over an agent you do not have an agent.'[233] But this too was an interpersonal judgement, as certain spies, particularly those motivated by ideology, were determined to be successful, a point reflected by Kuklinski's handlers who debated how to tell their agent to slow down his take: "we must be careful as to how we say this … we don't want him to think that his reporting isn't needed and greatly appreciated".[234] As with all bad news, setting down ground rules was an act best delivered face-to-face, not least when the agent desperately wanted to be valued.

However, even the most productive agents required an occasional morale boost. As the reality of their high stakes espionage took hold, it was not uncommon for agents to buckle under the pressure.[235] One way to address this problem was to give agents a boost of 'resilience' through 'psychological reinforcement'.[236] Means of psychological reinforcement varied depending on the personality of the agent; some handlers would attempt to boost moral with letters of encouragement, supportive gestures, or even gifts

[231] Ibid.
[232] Ibid, p. 161.
[233] Ibid.
[234] Weiser, B. *A secret life,* see chapter 9.
[235] Fischer, B. B. 'Fictitious spies and fake history', p. 171.
[236] Schmeidel, J. C. *Stasi: shield and sword of the party,* (London, Routledge, 2008), p. 122.

and remuneration.[237] But, nothing was more effective for relieving stress than personal meetings, allowing 'changes in the agent's attitude, motivation, personality, and health' to be observed.[238] They offered a human touch in times of high stress, as exemplified when Penkovsky's handlers photographed their agent in British and American military uniforms, thus satiating his belief that his own Soviet uniform did not reflect his ideological convictions.[239] As Gioe explains:

> …the decision to locate and clothe Penkovsky in two sets of formal military uniforms, a time consuming process, must be measured against the fixed amount of meeting time that may have produced an additional intelligence report or operational lead. Yet the team correctly believed that investing in Penkovsky's ego in this way would yield dividends in terms of his commitment to put his life on the line for the West.[240]

Similarly, although meetings with Tolkachev in Moscow were shorter and far more dangerous, their value could not be overlooked.[241] Despite ample gifts and substantial remuneration, and even begrudgingly supplying suicide pills (for emergencies) on his request, his handlers believed that Tolkachev had a "strong psychological need for direct personal contact".[242] He often arrived to meetings as a 'bundle of anxiety' to be unwound in a brief moment of emotional 'release'.[243] And Ogorodnik operated in Moscow for around a year before his handler was finally able to successfully arrange for a daring meeting, an event described by those involved in its planning as a 'seismic shift' and 'an immense morale booster'.[244]

---

[237] During a stand-down on personal meetings, Warsaw Station passed several encouraging personal letters to Kuklinski, who responded with "Your personal letters and the entire pertinent correspondence are for me a special kind of reward for tensions and anxieties, which, after all, I included in my thoroughly thought out and absolutely mature decision to initiate our cooperation". For more details, see Weiser, B. *A secret life,* see chapter 6.
[238] Wallace, R. et al. *Spycraft,* p. 422.
[239] Gioe, D. 'Handling HERO', p. 147; Duns, J. *Dead drop,* see chapter 4.
[240] Gioe, D. 'Handling HERO', p. 147.
[241] Royden, B. G. 'Tolkachev, a worthy successor to Penkovsky', p. 14.
[242] Hoffman, D. E. *The billion dollar spy,* see chapter 8.
[243] Ibid, see chapter 14.
[244] Mendez, A. et al. *The Moscow rules,* p. 75-76.

Owing to the numerous advantages of a personal meetings, most agents who could travel to friendly territory were handled predominantly by interpersonal tradecraft, allowing issues to be addressed as frequently as possible. In Penkovsky's first trip to London alone (one of several international visits), he safely met his handlers in hotels for 17 separate meetings, for a total of 50 hours.[245] Gordievsky would meet his handlers once a month in a London flat, scheduled conveniently for lunchtime, when KGB officers were expected to 'wine and dine' their contacts, meaning his absence would not be noticed.[246] And Ogorodnik would spend informal evenings with his handler in Bogotá's streets, 'drinking and talking about politics, philosophy, and personal interests'.[247] But in denied areas, namely Moscow, where surveillance teams held the advantage, meetings with agents 'were kept to a minimum, carefully planned, and never conducted without a specific reason'[248]

One case that exemplifies this point is Penkovsky's, who SIS decided to handle by personal meetings in Moscow due to a lack of alternatives.[249] Although Penkovsky already had a justifiable reason to meet Greville Wynne, as an SIS representative, he 'was not a professional intelligence officer', and could not 'be used too often without the KGB becoming suspicious'[250] Instead, feeling that personal meetings offered the least worst communication option, SIS chose Janet Chisholm, the wife of the SIS Station Chief, as Penkovsky's main liaison in Moscow.[251] SIS believed that as a

[245] Bower underscores the low level of risks involved in meeting Penkovsky while in the UK, noting how the first encounter 'initially took place at the Mount Royal hotel near Marble Arch', exactly where his Soviet delegation were staying, adding '[at] 9.45 p.m. on 20 April, after saying good night to the others of the Soviet delegation, Penkovsky silently left his own room and went by the back stairs to room 360.' In other words, the tradecraft involved in these operations was relatively low risk. For more details, see Bower, T. *The perfect English spy: Sir Dick White and the secret war 1935-90*, (London, Mandarin Paperbacks, 1996), p. 274; Gioe, D. 'Handling HERO', p. 145.
[246] Macintyre, B. *The spy and the traitor,* p. 134.
[247] Wallace, R. et al. *Spycraft,* p. 96.
[248] Ibid, p. 422.
[249] Gioe, D. 'Handling HERO', p. 148.
[250] Duns, J. *Dead drop,* see chapter 4.
[251] Corera, G. *The art of betrayal,* p. 155.

woman, Chisholm was unlikely to fall under KGB scrutiny, providing freedom to run so-called 'brush passes', brief encounters that could be held in public spaces such as parks and hallways.[252] To onlookers, it would seem as though Penkovsky had offered vitamin sweets to Chisholm's children in the park, but in actuality he was handing over concealed microfilms containing his intelligence.[253]

However, their reliance on Chisholm was fundamentally flawed (described by one Cold War writer as a "fit of intelligence lunacy"), since her identity was known to the former SIS officer, turned KGB spy, George Blake.[254] Furthermore, while one random encounter may have gone unnoticed, Penkovsky met Chisholm at least four times in the same park under the same pretext, bringing two people who should not have been seen together into the same space on multiple occasions.[255] Adding to these complications, Penkovsky may have been under KGB surveillance due to his deceased tsarist father.[256] By his own account, he always remained uncertain as to whether signs of mounting surveillance were a consequence of his espionage, or because the KGB simply did not trust him.[257] Either way, Penkovsky's meetings with Chisholm remains one of the key suspected factors in his final downfall.[258] And as far as the literature indicates, personal meetings of this frequency in Moscow would not be attempted again until Tolkachev was recruited two decades later.[259]

---

[252] Duns, J. *Dead drop,* see chapter 8.
[253] Ibid, see chapter 6.
[254] Ibid.
[255] Gioe, D. 'Handling HERO', p. 148-150.
[256] See Ashley, C. *CIA spymaster,* p. 217; Penkovsky, O. *The Penkovsky papers*, p. 248.
[257] Ibid.
[258] There is still a great deal of debate about precisely how Penkovsky fell under suspicion, and it remains unclear whether KGB surveillance was the cause of his downfall or simply a means of gathering evidence. For more details, see Berkeley, R. *A spy's London*, (Barnsley, Pen & Sword Military, 1994), p. 188-193.
[259] One known exception is Ogorodnik – his handler managed to pull off one meeting before the agent's arrest, and it required considerable planning – including a series of disguises, an identity swap, and an operative diving from a moving vehicle. For more details, see Mendez, A. et al. *The Moscow rules*, p. 70-75.

Without means to travel abroad, all of Tolkachev's meetings occurred in Moscow, often inside the agent's own car.[260] To avoid the mistakes made in the Penkovsky case, Moscow Station used an army of operatives who each performed lengthy surveillance detection runs, using decoy systems designed to throw off KGB tails.[261] In addition to a variety of disguises, and technical equipment designed to monitor KGB radios, the CIA also employed a system known as the 'Jack-in-the-Box'.[262] This innovative trick involved officers leaping from the passenger seat of a moving vehicle just as it turned a corner; a mechanical mannequin would spring up in their place, to confuse any tailing cars. For the KGB surveillance cars in pursuit, it would appear as though nobody had left the vehicle, allowing the escapee to continue their journey to Tolkachev unwatched.[263] Nonetheless, every meeting with Tolkachev carried enormous risks, and in periods of heightened surveillance (usually following a diplomatic fracas) meetings were routinely aborted or abandoned for lengthy periods of time.[264] And if one officer had failed to notice their tail, the mistake could have been fatal, leading surveillance teams straight to the agent.

However, although SIS chose to handle Penkovsky interpersonally because it lacked the tradecraft to communicate by safer means, by the time of Tolkachev it seemed increasingly possible to handle Moscow agents by *impersonal communications*. Not all aspects of handling, such as tasking and direction, required a personal touch, and in times of crisis intelligence often needed to be transmitted quickly.[265] Personal meetings required substantial planning, and were not easy to schedule in an emergency.

[260] Royden, B. G. 'Tolkachev, a worthy successor to Penkovsky', p. 20.
[261] For more details, see Ibid; Wallace, R. et al. *Spycraft*, p. 131.
[262] Mendez, A. et al. *The Moscow rules*, p. 115.
[263] Ibid.
[264] Hoffman, D. E. *The billion dollar spy*, see chapter 15.
[265] Gioe, D. V. 'The more things change': HUMINT in the cyber age', in *The Palgrave Handbook of Security, Risk and Intelligence*, edited by Robert Dover, Huw Dylan, and Michael Goodman (London, Palgrave, Macmillan, 2017), p. 221 & 223.

For example, Penkovsky's handlers 'listened with great interest … as [he] explained that he had known about the [Berlin Wall] plan four days in advance but had no way of contacting anyone urgently.'[266] Thus, *impersonal* communications offered a means to transmit intelligence quickly and to reduce burdens on personal meetings. However, in order to be viable, all impersonal tradecraft had to meet certain conditions; as Wallace et al explain, they needed to be 'SPAM proof':

> Secure: the message content must be unreadable to anyone other than the intended recipient ... they protect the meaning of a covert message, even if it should be intercepted.
>
> Personal: The message presence must be inaccessible to anyone other than the intended recipient. A loaded-brick concealment [provides] a host for secret messages that would appear uninteresting and normal for their environment. Only the intended recipient would know to look inside.
>
> Avoid traffic analysis: The existence of a communications link between the agent and handler must be hidden ... There must not be any record of clandestine activity ... to raise suspicion about the agent during a search.
>
> Mask the existence of the fact of communication: The fact that a communication is or has occurred must remain secret.[267]

Most two-way communications relied on car exchanges, dead drops (dead-letter boxes in British parlance), or secret writing, with either party notifying the other that a communication was ready through a variety of signals, such as chalk marks or angled curtains. [268] These would often work in tandem, depending on the nature of the content being sent and the options available to the agent. When Moscow Station finally agreed to work with Tolkachev, they first phoned his home from a phone both to provide the whereabouts of a dead-drop disguised as a discarded dirty mitten (the phone call itself being a dangerous act), which contained further instructions and equipment for sending

[266] Corera, G. *The art of betrayal,* p. 162.
[267] Wallace, R. et al. *Spycraft,* p. 450.
[268] Gordievsky, as a case in point, would signal his intent to begin exfiltration operations inside Moscow by standing in Kutuzovsky *prospect,* Moscow, while holding a Safeway bag and eating a Mars bar. For more details, see McCauley, M. *The Cold War 1949-2016*, (London, Routledge, 2017), p. 204-205; Weiser, B. *A secret life,* see chapter 3.

letters written in invisible inks.[269] That dead-drop allowed Tolkachev to respond with detailed answers to the CIA's questions, convinced Langley that a long-term operation was worthwhile, and allowed both parties to schedule their first meeting.[270] The dead-drop, in essence, allowed equipment to be exchanged, the secret writing allowed questions to be answered, and the meeting developed trust.

But the rudimentary systems honed throughout the early Cold War were hardly without risks. Car exchanges required packages to be quickly tossed from a still or moving vehicle to an agent stood on the street or inside their own car.[271] In Warsaw, intelligence officers would quickly pass packages to Kuklinski as they turned a corner, just far ahead of mobile surveillance teams to be out of view.[272] But akin to a personal meeting, each car exchange required substantial planning, perfect timing, and privacy from onlookers. The vehicle and the agent needed to be positioned in such a way that neither trailing surveillance cars nor passing pedestrians would notice, which was a complex task in Warsaw's bustling streets. When one intelligence officer identified only two suitable sites in Warsaw, headquarters described them as "too risky, dangerous, wouldn't work".[273] Their vulnerability was exemplified by the arrest of an agent named Filatov and his CIA contact, both of whom were spotted by KGB surveillance teams in the middle of an exchange.[274]

Dead-drops involved hiding packages in public spaces to be picked up later, but their popularity morphed into its own weakness.[275] Ideal hiding places required privacy and protection from the elements, but even in sprawling capital cities popular sites were

[269] Wippl, J. W. 'The CIA and Tolkachev vs. the KGB/SVR and Ames: a comparison', *International Journal of Intelligence and Counterintelligence,* 23:4, 2010, p. 640.
[270] Royden, B. G. 'Tolkachev, a worthy successor to Penkovsky', p. 8-10.
[271] Wallace, R. et al. *Spycraft,* p. 423.
[272] Weiser, B. *A secret life,* see chapter 3.
[273] Ibid.
[274] Hoffman, D. E. *The billion dollar spy,* see chapter 3.
[275] Corera, G. *The art of betrayal,* p. 136; Wallace, R. et al. *Spycraft,* p. 36 & 425.

often overused and staked out by observation posts, making fresh locations increasingly difficult to find.[276] Similar issues plagued Penkovsky's handling, who is often wrongly assumed to have been run by dead drops in Moscow; in reality, his SIS handlers felt that dead drops were simply too insecure for Moscow conditions, due to the threat of their accidental discovery.[277] CIA officers did try to place a drop for Penkovsky, but as Christopher Andrew's explains, it turned into farce:

> Hugh [Montgomery, the CIA's deputy chief of Moscow Station] …arranged for Penkovsky to be one of the Soviet officials invited to the 1962 Independence Day Party on 4 July 1962 at the US ambassador's residence in Moscow, Spaso House. Penkovsky was told to visit the rest room and leave [materials] in a waterproof container inside the cistern.
>
> Retrieving Penkovsky's container proved more difficult than [Hugh] had anticipated. He had expected the toilet to have the usual low-level US cistern. Instead, when he entered the rest room, he discovered that there was a cast-iron Russian cistern positioned above head height. When Montgomery tried to stand on the wooden lavatory seat, it broke and he found himself with one foot inside the toilet. Next he stood on the washbasin. Just as he retrieved the container from the cistern, the washbasin came away from the wall. By now rather bedraggled, Hugh decided not to stay for the rest of the reception. He told me that, just as he was leaving, he heard another guest complain that someone had trashed the restroom.[278]

Technological advances eventually made dead-drops easier to place and hide.[279] These included faux bricks that looked, felt, and weighed the same as real bricks, spiked dead-drops that could be buried in the ground, and even freeze dried animal carcasses which were combined with chemical formulas to make them unappetizing to stray animals (Wallace teased that millions of dollars were spent on identifying said formula, before OTS technicians settled on Tabasco sauce).[280] Advances in concealments allowed

[276] Wallace, R. et al. *Spycraft,* p. 36 & 425.
[277] Gioe, D. 'Handling HERO', p. 148-149.
[278] Andrew, C. 'Remembering the Cuban missile crisis: memoirs, oral history and lieux de mémoire' in An International History of the Cuban Missile Crisis: A 50-Year Introspective, edited by David Gioe, Len Scott and Christopher Andrew (London, Routledge, 2014), p. 19-20.
[279] Wallace, R. et al. *Spycraft,* p. 392; Bob Kovacs (3 March 2010) CIA gadgets and techniques with Bob Wallace – in HD, *Youtube.* Available at: https://www.youtube.com/watch?v=vQ7K52cvpyA [accessed 10 January 2018].
[280] Ibid.

Ogorodnik to be handled almost entirely by dead-drops while in Moscow, although it bears note that these did not resolve the need for substantial planning nor did they fully resolve the possibility of accidental discovery.[281] Indeed, threatening notes would be left inside the drops encouraging anyone who stumbled upon them to throw their contents in a nearby river (the notes would also be used to conceal secret writing) – but the fact remained that if a drop was found containing Ogorodnik's intelligence, he could have been swiftly incriminated.[282]

Alternatively, secret messages could be sent directly to the agent's address, hidden on postcards using invisible inks or microdots (specialised cameras that shrank photographs to the size of a grammatical period, allowing them to be hidden under stamps or within the body of the letter itself).[283] However, postal mail in the Eastern Bloc was heavily monitored by armies of astute censors trained to spot the vaguest signs of secret writing.[284] As Everett argues, 'it would not have taken a trained counter-espionage agent more than a few seconds to establish that the paper carried a secret message.'[285] Moreover, unlike dead drops and car exchanges, secret writing required incriminating equipment, 'being caught with a microdot camera or other secret writing equipment was basically an admission of espionage.'[286] Given these issues, and the fact that several agents were arrested after intelligence officers were observed mailing

[281] Mendez, A. et al. *The Moscow rules,* p. 51-57.
[282] Ibid.
[283] Everett, J. A. *The making and breaking of an American spy,* (Durham CT, Strategic Book Group, 2011), p. 65-66 & 70-71.
[284] Despite enormous levels of censorship, the KGB lacked the resources to check every single letter, leading the CIA to run numerous tests to determine their selection parameters. Nonetheless, secret writing was persistently insecure. For more details, see Macrakis, K. *Seduced by secrets,* p. 219-221; Wallace, R. et al. *Spycraft,* p. 63-65; Mitrokhin, V. *KGB lexicon: The Soviet intelligence officer's handbook*, (London, Frank Cass, 2002), p. 64.
[285] Everett, J. A. *The making and breaking of an American spy*, p. 65-66.
[286] Mendez, A. J. & McConnell, M. *The master of disguise*, p. 223.

letters posted to their addresses, messages sent by secret writing (at least when sent by mail) were largely avoided in hard target states.[287]

New opportunities began emerging in the 1970s, through advances in burst radio technology. Even by the early Cold War, one-way radio broadcasts were firmly cemented in espionage affairs, with 'numbers stations' around the globe broadcasting coded messages to anyone with a commercial receiver. [288] The agent would listen for these numbers at prearranged times and dates, and decrypt them using a cipher system called the one-time pad.[289] While two-way communications were too insecure for agents in Moscow (because the *sender* could be located through directional antennas), by only *receiving* the communication the agent was invulnerable to being traced.[290] There was an underlying threat that eavesdroppers might crack the code - a prospect turned into harsh reality for Soviet and East German spies who were compromised by coding errors and American super computers – but the one-time pad largely remained a reliable source of security for the West's spies.[291]

But in the 1970s, OTS spent millions of dollars (nearly bankrupting its office) to build a ground-breaking radio communication device called SRAC (Short Range Agent

[287] Weiser, B. *A secret life,* see chapter 3.
[288] Schmeidel, J. C. *Stasi,* p. 128.
[289] Ibid.
[290] While it is commonly argued that the Soviets preferred HUMINT over TECHINT, contradictory evidence suggests that the Eastern Bloc ran a vast interception empire. Herman, for example, cites an academic paper from 1989 that shed a contradictory light on the full extent of Soviet interest in technical intelligence. It claimed "the Soviet Union maintains by far the largest Sigint establishment in the world", one that was 'said to be fives time the size of the US establishment'. For more details see Herman, M. *Intelligence power in peace and war,* (Cambridge, Cambridge University Press, 1996), p. 68; Maddrell, P. *Spying on science,* p. 244; Bury, J. 'Finding needles in a haystack: the Eastern Bloc's counterintelligence capabilities', *International Journal of Intelligence and Counterintelligence,* 25:4, 2011, p. 761; Bury, J. 'From the archives: the U.S. and West German agent radio ciphers', *Cryptologia,* 31:4, 2007, p. 343. Macrakis, K. *Seduced by secrets,* p. 195.
[291] Early in the Cold War, the Soviets unknowingly injected repetitions into their one-time pad ciphers, allowing Western analysts to decrypt broadcasts, culminating in a counterintelligence windfall known as the Venona project. However, in the later Cold War, supercomputers allowed the Americans to decrypt East German signals, leading to the arrest of a senior ranking West German official known as Günter Guillaume. He was exposed because the East German's had a habit of broadcasting birthday wishes to their agents, with the date of the communication providing sufficient information to narrow the list of suspects. For more details, see Pincher, C. *The truth about dirty tricks: from Harold Wilson to Margaret Thatcher,* (London, Sidgwick & Jackson Ltd, 1990), p. 325; Schmeidel, J. C. *Stasi*, p. 134.

Communications). As Mendez et al argue: '[SRAC] was truly revolutionary – a two-way burst transmitter that could send and receive fifteen hundred securely encrypted characters in less than five seconds at the touch a button.'[292] The first device, named Buster, which was about the size of a pack of cigarettes, could either send messages to intelligence officers holding receiving units in the streets, or to base stations in US embassies.[293] Polyakov was one of the first agents to use SRAC inside of Moscow, transmitting his messages to a receiving station inside the US embassy while he passed the building by foot, bus, car or bicycle.[294] Once Polyakov's messages were received, the base station 'replied with a confirmation signal and transmitted its own preloaded, though more limited character set, back to the agent's unit.'[295] With the aid of SRAC, Polyakov was supposedly able to maintain contact with his handlers for years while posted in Moscow, keeping Langley updated on internal GRU affairs.[296] But although the device was a technical leap, it was not without risks. At minimum, it was blatant and highly incriminating spy gear, unlike anything on the commercial market, and it also required awkward operational acts, as Hoffman explains:

> … an agent would have to be looking down into his pocket until the red verification light flashed, or else he would not know the message went through. The red light flashed only after a pause. Was peering into one's pocket, watching for the light to flash, the kind of body language that would give away an agent? Was it worth the risk?[297]

[292] A somewhat more primitive system of burst transmissions began with the tape recorder, as Maddrell explains: 'the Americans and French gave their spies tape recorders on which they were to record their messages. The tape recorders played what was recorded fast, enabling the spies to transmit a [radio] message fast—ten times faster than normal. This made it difficult for the MfS to determine where the transmission had been made', for more details, see Mendez, A. et al. *The Moscow rules*, p. 85; Maddrell, P. *Spying on science*, p. 244; Wallace, R. et al. *Spycraft,* p. 115.
[293] Wallace, R. et al. *Spycraft,* p, 115-116.
[294] Ibid.
[295] Ibid, p. 116.
[296] West, N. *Historical dictionary of international intelligence*, (London, Rowman & Littlefield, 2015), p. 277.
[297] Hoffman, D. E. *The billion dollar spy*, see chapter 8.

Moreover, when the Eastern Bloc eventually learned about SRAC's existence, apparently with the aid of their Cuban allies, they developed means to detect and triangulate its transmissions.[298] Kuklinski, who received an SRAC unit named Iskra, was instructed to avoid sending too many message to the US embassy in Warsaw, out of concerns that technical listening equipment would be nearby.[299] His handlers concerns proved apt, as following Cuba's intelligence, Polish security services did detect signals around the US embassy, mounting a manhunt for an agent suspected of operating within 100 meters of the compound.[300] The entire vicinity was surrounded with physical and technical observation equipment, in an operation that cost Polish security services around one million dollars.[301] Even if counterintelligence were unable to pinpoint the area of transmission, everyone within the vicinity could have been stopped and searched, potentially exposing the agent.

Whereas SRAC required agents to get in close proximity to intelligence officers or US embassies, satellite communications allowed messages to be sent from almost anywhere. In the 1960s, the CIA introduced its first satellite uplink named Birdbook, which proved too impractical for Moscow conditions.[302] Successful Birdbook transmissions depended on the agent carrying a bulky piece of incriminating equipment (the size of a briefcase) to an area with a clear line of sight, such as a rooftop.[303] And the process had to be completed in around five minutes, allowing the agent to connect with the satellite arcing across the sky and escape before the KGB detected the signal and arrived at the scene.[304] But technological advances soon reduced the size of

[298] Bury, J. 'Project Kalina', p. 122.
[299] Weiser, B. *A secret life,* see chapter 9.
[300] Bury, J. 'Project Kalina', p. 125.
[301] Ibid
[302] Richelson, J. T. *Wizards of Langley*, p. 187
[303] Ibid.
[304] Ibid; Wallace, R. et al. *Spycraft,* p. 441.

equipment and improved transmission, leading Langley to recommend that Tolkachev use its latest system "for *all* communications in between personal meetings."[305] Their reasoning was based on fears that tensions in the USSR were pointing towards the closure of Moscow Station, potentially eliminating means to communicate with their agent during a crisis. Hence, a direct link to the US Marisat satellite network offered an ideal opportunity to improve Tolkachev's security while ensuring a line of communication should CIA operatives need to be evacuated from the city.[306]

Tolkachev's handlers, however, held "serious reservations" about the satellite uplink.[307] Moscow lay on the very outer edges of the Marisat satellite network, meaning the device, known as RS-804, had never been successfully tested from inside the city.[308] After further failed tests (not by Tolkachev), Langley reconsidered its proposals, concluding that satellite uplink was an ill-fitting choice.[309] Had it worked, satellite uplink still required incriminating equipment and proved vulnerable to technical triangulation.[310] When the Eastern Bloc learned of RS-804's existence, again with the aid of Cuban intelligence, they immediately developed systems to detect and trace its transmissions.[311] Near the end of the Cold War, they mounted a considerable SIGINT effort, intercepting 250-350 Marisat transmissions per month.[312] In East Germany, the Cuban's findings allowed MfS to confirm that no RS-804 transmissions were being made within the country, and it even led to the discovery of CIA technical collection

[305] Hoffman, D. E. *The billion dollar spy*, see chapter 12.
[306] Ibid.
[307] Ibid.
[308] Crypto Museum – RS-804: US satellite spy radio set. Available at: https://www.cryptomuseum.com/spy/rs804/index.htm [accessed 12 March 2019]
[309] Hoffman, D. E. *The billion dollar spy*, see chapter 12.
[310] Bury, J. 'Project Kalina', p. 120-125.
[311] Fischer, B. B. 'Deaf, dumb, and blind: the CIA and East Germany', in *East German Foreign Intelligence: Myth, Reality and Controversy*, edited by Kristie Macrakis, Helmut Muller-Enbergs, and Thomas Wegener Friis, (Abingdon, Routledge, 2010), p. 59.
[312] Bury, J. 'Project Kalina', p. 120-124.

sensors that were using the same frequencies as the satellite uplink.[313] And even Polish security services, who held relatively inferior SIGINT systems, were able to detect and narrow the origin of RS-804 signals to around 40-100km, confirming that an agent was operating in the 'Tricity' region of the Baltic Sea.[314]

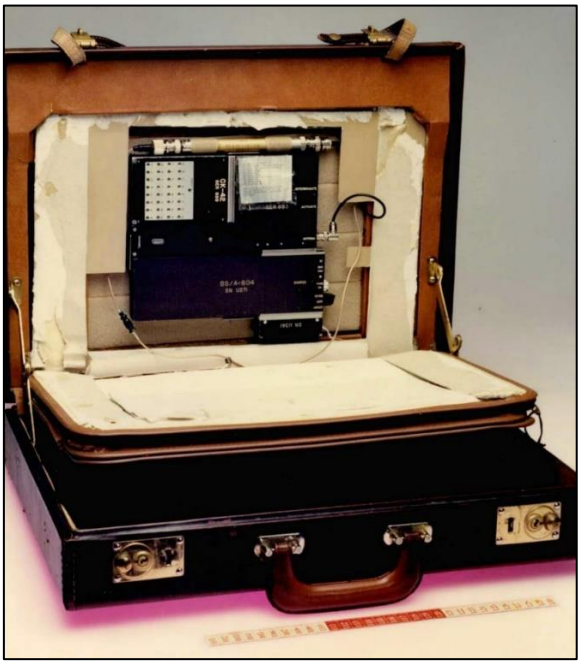

Figure 2: A captured RS-804 satellite-uplink.[315]

In essence, every method of communication, whether by interpersonal or impersonal means, carried unique risks, which in turn increased the need for trust by handling officers. At minimum, some agents felt uncomfortable about certain methods at their disposal, meaning handlers needed assurances that communication tradecraft was likely to be embraced. Penkovsky requested not to be handled by personal meetings while in Moscow, preferring the security of an impersonal communication, but his decision was overruled by SIS.[316] Kuklinski, on the other hand, asked his handlers whether he should carry his gun to each car exchange, fearing that something

[313] Fischer, B. B. 'Deaf, dumb, and blind', p. 59.
[314] Bury, J. 'Project Kalina', p. 124
[315] Crypto Museum – RS-804: US satellite spy radio set. Available at: https://www.cryptomuseum.com/spy/rs804/index.htm [accessed 12 March 2019].
[316] Gioe, D. 'Handling HERO', p. 148.

might go wrong.[317] In fact, slightly riled after one close call with Polish surveillance, Kuklinski later apologised to his handlers for not responding to CIA officers who had offered a quiet greeting during one such exchange, stating "the tensions during these few moments is so strong that words of sentiment such as I would like to express remain somewhere in the background".[318] Tolkachev also described dead drops as "psychologically" burdening, because he was leaving incriminating information in an open environment.[319] Instead, he reasoned that since his handlers had to lose their surveillance tails to access dead drops anyway, they might as well meet face-to-face.[320]

While some agents were prepared to use certain methods despite their concerns, others were less amenable, one Czech agent 'absolutely refused to use dead drops' because incriminating messages would be 'out of his hands'.[321] Similarly, Sheymov refused to use radios, dead drops, car exchanges, or any method other than personal meetings.[322] He told his handlers that during a KGB briefing he was shown a list of agents caught while performing their communication tradecraft, "[and] you know what? Out of all of them – dozens – there was no mention of anyone being caught in a personal meeting".[323] He reasoned that because personal meetings were exceptionally dangerous, intelligence officers were more likely to pay careful attention to their tradecraft, reducing the chances of a mistake. And despite attempts to convince him otherwise, including by making the point that personal meetings would delay his defection considerably, his CIA handler eventually conceded, "[all] right, it's your neck after all. We'll do everything in our power to help you and to assure your security".[324]

[317] Weiser, B. *A secret life,* see chapter 4.
[318] Ibid, see chapter 5.
[319] Royden, B. G. 'Tolkachev, a worthy successor to Penkovsky', p. 14.
[320] Ibid.
[321] Hoffman, D. E. *The billion dollar spy,* see chapter 1.
[322] Sheymov, V. *Tower or secrets,* p. 371.
[323] Ibid.
[324] Ibid.

Given Sheymov's exceptionally high value as a cipher clerk, his handlers were willing to accept his risky conditions, albeit personal meetings did offer an opportunity to try to convince him otherwise.

But even if the agent trusted their tradecraft, the handler also needed trust in their agents' capabilities. Everett raises this issue with secret writing, noting that a single mistake required messages to be resent, doubling the odds of exposure.[325] CIA officers struggled to read one letter sent by Ogorodnik, who botched his message by writing on waxed paper, with the wax dissolving in chemical processing alcohol and blurring much of its contents.[326] Microdots, while in some ways simpler than invisible inks, were often so well hidden by agents as to be unlocatable by the recipient, or too poorly hidden so as to detach in transit.[327] Moreover, careless use could also expose the agent to their own family, a point underscored when Everett, a trained CIA officer, blew his cover to his own daughter when she abruptly entered the bathroom where he was processing a newly arrived letter.[328] Tolkachev experienced similar issues with his one-way radio sets, finding it difficult to listen to radio broadcasts without arousing suspicions in his family household. [329] He eventually returned his radio sets having never used them, as he was 'unable to securely monitor these broadcasts' due to the constant presence of his wife and son.[330] Therefore, as the risks mounted, handlers required a certain level of confidence that agents would be sensible, applying their tradecraft carefully and with discretion.

[325] Everett, J. A. *The making and breaking of an American spy*, p. 68-69.
[326] Mendez, A. et al. *The Moscow rules,* p. 73.
[327] Everett, J. A. *The making and breaking of an American spy*, p. 71; Wallace, R. et al. *Spycraft,* p. 429-431.
[328] Everett, J. A. *The making and breaking of an American spy*, p. 215-216.
[329] Royden, B. G. 'Tolkachev, a worthy successor to Penkovsky', p. 21.
[330] Ibid; Wippl, J. W. 'The CIA and Tolkachev vs. the KGB/SVR and Ames', p. 641.

This need for trust in the agent's sensibilities was only magnified by more expensive capabilities such as SRAC and satellite uplink. Polyakov's success in Moscow with SRAC was largely derived from the amount of time he spent training with the device while posted in India, but not all agents were afforded the same luxury.[331] When Langley suggested giving SRAC to Tolkachev, his handlers disagreed, stating that they had "no opportunity for training or practice", and that given his preference for interpersonal contact, they seemed to have "more to lose than to gain".[332] The Station chief, Hathaway, disagreed, having heard of SRAC's success with another untrained agent, Kuklinski, in Warsaw.[333] Kuklinski was given SRAC with twenty pages of instructions, and told he could send "information of extraordinary importance and urgency … that cannot wait even for a few hours."[334] Tolkachev, as such, was given an SRAC named Discus, and similarly told in no uncertain terms to "read the instructions".[335] In either case, Tolkachev and Kuklinski's handlers required a certain degree of confidence that their agents, without opportunity for training, could use this equipment without endangering themselves.

But trust wasn't just about the agent's perceived competencies (especially if they had no opportunity for training) it was also about the agent's loyalties. Unwittingly giving valuable technology to a double agent could allow counterintelligence to develop a countermeasure, which is exactly what happened with SRAC and satellite uplink.[336] It is not entirely clear how the Cuban's first learned about SRAC, but former CIA analyst Brian Latell claims that all Cuban spies recruited in this period were in fact double agents, suggesting that SRAC may have been given to a duplicitous Cuban

[331] Wallace, R. et al. *Spycraft,* p, 115-116.
[332] Hoffman, D. E. *The billion dollar spy,* see chapter 8.
[333] Ibid, see chapter 12.
[334] Weiser, B. *A secret life,* see chapter 9.
[335] Royden, B. G. 'Tolkachev, a worthy successor to Penkovsky', p. 21.
[336] Bury, J. 'Project Kalina', p. 123-126.

asset.[337] Likewise, two incidents gave the West's opponents access to an RS-804 satellite uplink unit. The first occurred when a CIA officer was arrested while testing the device in a Moscow park.[338] The officer, Richard Osborne, was supposedly oblivious to the fact that he was being watched around the clock by KGB surveillance teams, who were lying in wait for him to make a transmission.[339] This situation was worsened two years later, when Cuban intelligence received another RS-804 unit from a double agent whom the CIA mistakenly trusted, whose betrayal allowed Havana to then develop countermeasures which were shared with their Eastern Bloc allies.[340] As such, the delivery of an RS-804 satellite uplink to an untrustworthy agent, then led to technical countermeasures that created further risks for other agents. To sum up, as the risks mounted in communication tradecraft, it is clear that handlers had to be increasingly mindful of agents justifiable concerns for safety, but also more cognizant of their agents competencies and loyalties.

Collection

Ultimately all agents were recruited for the purpose of collecting secret information, but agents who regularly produced high quality intelligence were also far more likely to be trusted.[341] Bagley notes how Polyakov's handler was convinced he was dealing with a 'KGB plant' during the early stages of their relationship, until 'dramatic improvements' in the quality of Polyakov's production swayed his mind.[342] However, spies were rarely tasked to break into guarded vaults, instead they were expected to collect information

[337] Latell, B. *Castro's secrets: the CIA and Cuba's intelligence machine*, (New York, Palgrave, 2012), p. 15.
[338] Crypto Museum – RS-804: US satellite spy radio set. Available at: https://www.cryptomuseum.com/spy/rs804/index.htm [accessed 12 March 2019].
[339] Ibid.
[340] Fischer, B. B. 'Deaf, dumb, and blind', p. 59.
[341] Wallace, R. et al. *Spycraft*, p. 366.
[342] Bagley, T. 'Ghosts of the spy wars: a personal reminder to interested parties', *International Journal of Intelligence and Counterintelligence*, 28:1, 2015, p. 7

within their working purview, minimising the threat of exposure.[343] That said, some agents, such as Penkovsky, tried to push the limits of their access to increase their value, taking inordinate risks in the process.[344] Penkovsky routinely visited Soviet Ministry of Defence archives, and as the *Penkovsky Papers* note, 'it is reasonable to assume that somebody may have seen him in the library and … made a note on his file.'[345] Tolkachev took similar risks, acquiring documents that fell well beyond his working needs, as he wrote to his handlers:

> The number of documents drawn by me greatly exceeds my productive needs. For example, I will never be able to explain why I needed the technical descriptions of the AVM RLS RP-23, N-003, N-006, N-005 . . . This is also hard to explain because our laboratory has stopped overseeing the RLS RP-23, N-003, N-006 in September, 1978, and our laboratory was never even involved in issuing the documentation for the RLS N-005 or its serial introduction. The listed considerations induce me, already for the third time, to turn to you with the request that I be passed the means of self-destruction at once.[346]

These technical numbers relate to documents of value, but by signing each out with his name he left a paper trail that could easily have been traced back to him, 'if the KGB ever for any reason suspected that information was being leaked on the research activities on which he was working, a review of the document sign-out permission cards would quickly finger him as the leading suspect.'[347] This also explains the 'means of self-destruction' - simply put, Tolkachev wanted a suicide pill for insurance should anyone notice his irregular patterns of access.[348]

Even if agents could acquire permission to access documents, they still needed means to remove them. During the earlier years of the Cold War, agents such as

[343] Copeland, M. *The real spy world*, p. 119-122.
[344] Penkovsky, O. *The Penkovsky papers*, p. 232-233.
[345] Ibid.
[346] Hoffman, D. E. *The billion dollar spy*, see chapter 8.
[347] Ibid; Royden, B. G. 'Tolkachev, a worthy successor to Penkovsky', p. 19.
[348] Hoffman, D. E. *The billion dollar spy*, see chapter 8.

Penkovsky would take documents home to be copied in privacy.[349] But taking them home was never a simple process, a point exemplified when Tolkachev's institution implemented new security procedures:

> Previously, he could check out classified reports from the First Department by signing for them on a permission sheet that remained on file with the department. At lunchtime, he could conceal the documents in his coat, leave the building, photograph them at home when he was alone, return to the institute after lunch, and put the documents back. At the main gate, where he showed his building pass, they would rarely check whether he was carrying anything.
>
> Now … in order to check out documents from the First Department, he was required to leave his building pass with the clerks in that department. Without the pass, he could not leave the building at lunch nor photograph secret documents at home. The only documents he might be able to take home were less sensitive technical journals … he was facing a big setback; his usual habit of just walking out with documents in his coat pocket was not going to be possible.[350]

While Tolkachev was given a forged permission slip to take documents home, another review of internal security procedures made the pass redundant, leaving the agent without any means to collect intelligence except by taking photographs or notes inside his office.[351] Furthermore, the Soviets, akin to any secure institution, clamped down on potentially harmful technology in the workplace; photocopiers, as a case in point, were often guarded under lock and key, to protect misuse by internal spies.[352] Tolkachev explained that his workplace photocopier was "located in a special room and operated by four or five employees … Entry to the copying room is not allowed to persons not working there."[353] And while commercial office tools spread throughout the working world, those luxuries were often unavailable to those who worked with classified

[349] Duns' notes that in Penkovsky's trial, evidence provided included a surreptitious photo of Penkovsky taking photographs of documents with a Minox camera while at home. However it bears note that since he had already been arrested, the photograph may have been staged. For more details, see Duns, J. *Dead drop*, see chapter 14.
[350] Hoffman, D. E. *The billion dollar spy*, see chapter 8.
[351] Another factor that complicated Tolkachev's espionage was his lack of privacy at home, meaning many of his documents would need to be copied within the workplace. For more details, see Ibid, see chapter 5 & 14; Royden, B. G. 'Tolkachev, a worthy successor to Penkovsky', p. 17.
[352] Copeland, M. *The real spy world*, p. 131-132
[353] Hoffman, D. E. *The billion dollar spy*, see chapter 7.

information.[354] Copeland, for example, describes how spies began adopting portable office scanners to copy documents discreetly at their own desks, until astute security officers banned their use in secure establishments.[355]

With the exception of painstakingly taking notes (which is problematic when dealing with hundreds of detailed documents), many agents depended on clandestine photography to collect their take, a point personified by the legacy of the Minox, a small, affordable camera marketed under the slogan "not just for beautiful spies".[356] But the Minox was far from suitable for spies in bustling office environments, and it was given to Penkovsky not out of convenience but due to a lack of safer alternatives.[357] One issue was that for Soviet officials, being found with cameras of British and American origin, especially inside a secure institution, 'was about as incriminating as evidence could get'.[358] Furthermore, commercial cameras such as the Minox were notable for their noisy shutters, meaning they 'could not be easily used without others noticing'.[359] Realising the need for a more secure solution, Langley eventually designed a concealable, subminiature camera for use in high security offices, one built to meet very specific conditions:

> In addition to being able to capture high-resolution images of a full page without distortion at the edges or benefit of flash, the camera needed a film capacity of at least a hundred frames and a silent shutter system. Added to this, the camera had to be small enough to conceal in an item that a person would normally carry with them into guarded and secure facilities.[360]

The end product was a technical leap, the world's smallest point-and-shoot camera, about one sixth the size of a Minox and small enough to conceal inside a range of

[354] Copeland, M. *The real spy world*, p. 131-132
[355] Ibid.
[356] Young, S. *Minox: Marvel in miniature,* (Bloomington, AuthorHouse, 2000), p. 27-28.
[357] Wallace, R. et al. *Spycraft,* p. 37.
[358] Macintyre, B. *The spy and the traitor,* p. 78.
[359] Hoffman, D. E. *The billion dollar spy,* see chapter 7.
[360] Wallace, R. et al. *Spycraft,* p. 89.

personal items, such as watches, pens, or cigarette lighters. Known as the T-100 (and later, the T-50) it offered game-changing advantages.[361] At one point, SIS even tried to procure the camera for Gordievsky:

> MI6 was still using the old-fashioned Minox camera. The CIA, however, was known to have recruited a Swiss watchmaker to develop an ingenious miniature camera hidden inside an ordinary Bic cigarette lighter, which could take perfect photographs when used in conjunction with a length of thread, 11¼ inches long, and a pin. Using a piece of chewing gum, the thread was stuck to the bottom of the lighter; when the pin at the end lay flat on a document, that measured the ideal focal length, and the button on top of the lighter could be pressed to click the shutter. The pin and thread could be hidden behind a lapel. The lighter looked entirely innocent. It even lit cigarettes. This would be the ideal camera for Gordievsky.[362]

The supposition that Gordievsky could photograph reams of intelligence in a KGB *rezidentura* underscores the T-100's value.[363] However, these cameras were not without issues. Due to their size and complexity, each model held a limited film capacity and required a specialist touch to replace used batteries, meaning multiple cameras needed to be delivered at a time.[364] In fact, the KGB found five T-50s in a dead-drop loaded for Ogorodnik by the ambushed CIA officer, Martha Peterson.[365] As such, the agent was required to hide not only one highly incriminating camera, but an entire batch. Furthermore, because the cameras lacked a viewfinder and a flash, they were difficult to use in office environments.[366] The agent would need to find an environment with sufficient lighting, and clasp the concealed camera in a steady position above whatever document they were photographing.[367] Ogorodnik, as a case in point, would need to 'position his elbows on the table, hands together, and aim the pen down toward the

[361] Ibid, p. 89-90.
[362] Macintyre, B. *The spy and the traitor,* p. 203.
[363] Ibid.
[364] The T-100 held one-hundred frames (or photos) and the T-50 held fifty, with the later models having a smaller film capacity to improve overall reliability. For more details, see Wallace, R. et al. *Spycraft,* p. 89-90.
[365] Ibid, p. 98-100.
[366] Ibid, p. 90; Hoffman, D. E. *The billion dollar spy,* see chapter 8.
[367] Hoffman, D. E. *The billion dollar spy,* see chapter 7.

document. Eleven inches from the page was the perfect distance'.[368] This became problematic when agents were supposed to be photographing hundreds of documents, since constantly hunching over their desks in the same position while clasping an object risked arousing their colleague's attention.[369]

Once again, these risks pushed up the need for handlers to trust their agents, including to ensure that they would even use the risky tools given to them. Akin to the issues faced in covert communications, some agents were less keen to make the most of incriminating cameras, meaning their application in the field could have amounted to an unnecessary risk. For example, despite SIS's attempts to acquire one of the CIA's subminiature cameras for Gordievsky, he actually refused to use any type of camera – clandestine or not – inside his rezidentura, believing that the gains in terms of his production were vastly outweighed by the risks of being caught with such an incriminating piece of equipment.[370] Indeed, when offered, Gordievsky incorrectly assumed that the camera was being forced on him:

> When the British started to suggest secret photography, I said, 'Look, is there some demand from London for this? Do you have a norm of the number of devices that have to be in use? Because if you do, I'll accept one, and we can pretend I'm using it just to make life easier for you.' When they saw what I was getting at, they burst out laughing, and I felt embarrassed at having revealed how ignorant I still was of Western mental attitudes.[371]

But even if the agent was willing, the handler still needed ample trust in their agent's competencies. At minimum, giving incriminating cameras to an agent meant having confidence that they would keep those cameras hidden, a mistake made by Tolkachev whose espionage career was first discovered by his wife when she found a Pentax camera and balancing clamp hidden in his drawer.[372] Moreover, since most agents were

[368] Ibid.
[369] Ibid, see chapter 14.
[370] Gordievsky, O. *Next stop execution,* chapter nine.
[371] Ibid.
[372] Hoffman, D. E. *The billion dollar spy,* see chapter 7.

not professional photographers and documents needed to be as clear as possible, they required training.[373] Penkovsky, who proved to be naturally talented, required only a brief amount of training with the Minox camera while in London.[374] Ogorodnik, on the other hand, required weeks of training to prepare for his upgraded T-50.[375] While in Bogota, he would sneak 'away for small blocks of time that did not disrupt his normal pattern of activity or catch the notice of the KGB', with each session lasting somewhere between fifteen minutes and two hours.[376] Even with training, he struggled to photograph one highly valuable document while being monitored by a vigilant security guard, telling his handler: "[after] I get to the room, a guy walks behind me. I couldn't use the camera … [you] know what will happen if I make a mistake".[377] But when he finally managed to take the photographs, his training clearly paid off, with only two frames out of fifty distorted.[378] This achievement was not to be discounted, since photographing a document in a KGB vault under the nose of a watchful guard was something 'that had never been done before'.[379]

Moscow Station was far more hesitant to give Tolkachev a T-50 named Tropel, because he was 'untrained and untested'[380] As headquarters noted in a memo, giving Tropel to an agent who had no opportunity for training was "an extremely risky endeavour, and would require tremendous discretion and caution by [Tolkachev], and is not likely to help his blood pressure, either". Instead, he was first given a camera called Molly, a device he found to be disappointing, which was later followed by the commercial Pentax. Langley did, in the end, decide to give Tolkachev the Tropel, but

[373] Mendez, A. et al. *The Moscow rules,* p. 83.
[374] Duns, J. *Dead drop,* see chapter 4.
[375] Wallace, R. et al. *Spycraft,* p. 93-94
[376] Ibid.
[377] Ibid, p. 95.
[378] Ibid.
[379] Mendez, A. et al. *The Moscow rules,* p. 48.
[380] Hoffman, D. E. *The billion dollar spy,* see chapter 7.

'with the caution that they were only for "testing" at home; he should not risk taking them to the office'.[381] Herein, however, lay an even greater problem, because agents who were determined to be productive were more likely to take unnecessary risks.[382] Tolkachev much preferred the commercial Pentax over the Tropel, because it allowed him to take hundreds of high quality shots with relative ease, but whenever workplace restrictions prevented him from taking documents home he would try to smuggle the Pentax into work, taking photos at his own desk.[383]

This was an incredibly dangerous act, and when he destroyed his Pentax cameras during a security scare, Moscow Station refused to issue a replacement.[384] Instead, his handlers decided to offer more Tropel cameras, fearing that if they didn't provide a photographic capability, Tolkachev, who was dismayed by the idea of taking notes, might take further risks by buying himself another commercial camera. Without safer alternatives, Tolkachev took his Tropel shots in a men's bathroom, where poor lighting made many of his shots illegible, but his handlers considered this a favourable option compared to letting him loose with the Pentax.[385] In a similar case, when Polyakov decided to photograph an extremely valuable document (dubbed the "Kapitsa Document"), he held little confidence in his CIA 'rollover camera'.[386] Distrustful of the CIA's device, he decided to take another round of shots using a more basic 35-mm camera, one that produced a loud shutter noise that could have attracted his code clerk 'only a few feet away'.[387] His concerns were not entirely unfounded however, since of all the photographs he took, the roll over camera produced only one legible shot, while

[381] Ibid.
[382] Ibid.
[383] Royden, B. G. 'Tolkachev, a worthy successor to Penkovsky', p. 27.
[384] Ibid, p. 29.
[385] Ibid.
[386] Grimes, S & Vertefeuille, J. *Circle of treason,* see chapter 4.
[387] Ibid.

his preferred camera, a Soviet device, produced perfect shots.[388] Nonetheless, it underscores the point that regardless of the tools at their exposal, some agents preferred to be productive, even at the expense of endangering their own lives. As with handling, increased risks in collection pushed up the agent's need for trust in technology, but also exacerbated the operative's need for trust in their source, a factor that became all the more important if the agent was inclined towards maximising their production.

Evaluation

In the introduction to his book on the early history of MI5, Kevin Quinlan remarked that 'for all the technical developments that have aided intelligence collection over the last century, one basic element remains the same: people'.[389] In this context, Quinlan appears to be referring to the importance of manipulating and controlling human frailties and emotions for espionage purposes, but what this chapter has shown is that human behaviour is just as important to influencing tradecraft, as tradecraft is to allowing human behaviour to be exploited. In other words, the human dimension was a deciding factor throughout every aspect of espionage, ultimately determining whether methods succeeded or failed. Whether it was due to a lack of trust in technology, or to the unpredictability of the third party at the other end, the prospective or serving spy's behaviour always dominated tradecraft's outcome.

This is clearly apparent in the recruitment stage, where convincing fearful Soviet citizens to commit treason against the state was mired by the absence of privacy. Despite their advantage, personal meetings were extremely hazardous inside of Moscow, but so too were alternative forms of social communication. Telephones within

[388] Ibid.
[389] Quinlan, K. *The secret war between the wars: MI5 in the 1920s and 1930s* (Rochester, NY, The Boydell Press, 2014), p. xvii.

the capital were tapped around the clock, while outside Soviet borders the personal and work phones of Eastern Bloc officials remained highly susceptible to eavesdropping. Consequently, since the intelligence officer couldn't openly advertise their recruitment intentions without raising alarms, the safety of their relationship depended on their target's sensibilities. If the source telephoned from an insecure line, their connection to a foreign operative could be exposed and potentially ended. The only element that worked to the recruiter's favour was the Soviet tendency towards telephonic self-censorship, in the sense that there was a mutually unstated desire for discretion, one that limited the use of telephone calls.

Similarly, sources who chose to volunteer their services avoided the need for a long drawn out cultivation period, but the lack of access to safe communications encouraged even greater self-restraint. Anyone who wanted to volunteer their services from inside Moscow needed the common sense to avoid physically entering or telephoning surveilled embassies. However, even by using marginally more secure alternatives, including chasing cars or requesting the aid of foreign students, Soviet volunteers faced a critical dilemma - on the one hand, they knew that the methods they relied upon were inherently dangerous, yet on the other hand, they were obliged to supply incriminating bona fides if their dangerous pitches were ever to be taken seriously. In that sense, only if the volunteer was prepared to take an enormous gamble, and understood the means of securing a response, was a pitch likely to succeed.

Efforts to build such confidence in sources, even to the point of being able to conduct 'cold pitches' were, however, vastly aided by prior surveillance. Given the difficulties entailed in running large surveillance operations, audio listening devices often offered a more reliable and invasive form of eavesdropping. Embassies made for appealing targets, since their vibrant environments were almost guaranteed to produce

some actionable results. In addition to the collection of diplomatic intelligence, the day to day affairs of numerous Soviet officials offered abundant potential recruitment data. Yet, against high security establishments, the planting of listening devices was generally prohibitively risky. The targeting of Soviet officials in their apartments or hotels offered greater leeway, not least because the risks of surreptitious entry, at least abroad, were substantially reduced. However, the risks of breaking into a premises had to be weighed against the likelihood that targets would say at least something of importance. And yet those odds were only dampened by an ingrained fear among Soviet officials of eavesdropping by the KGB.

Given these issues, recruitment heavily depended on a handful of opportunities, few of which ever occurred in Moscow. Handling was permeated by the constant fear of deception and the need to stabilise the agent's psychological wellbeing. While the cultivation of interpersonal bonds could increase trust between the parties, this proved problematic in Moscow conditions. Even with a cooperative agent, personal meetings were extremely hazardous, increasing reliance on impersonal communications. However, all forms of impersonal tradecraft carried differing risks, each weighing heavily on the mindset of some agents, and leading intelligence officers to question their suitability for more concerned assets. Although advances in burst radio technologies opened safer opportunities, not least through the highly popular Short Range Agent Communications (SRAC) device, these were troubled by issues of trust. A duplicitous or clumsy source could deliver top tier spy gear into the hands of opposing counterintelligence, who might then develop a countermeasure. Consequently, the most secure tools were reserved for trusted and tested agents, limiting their use in the early stages of handling.

An agent's ability to exfiltrate large volumes of information strengthened their overall value and consolidated their handler's trust. A productive source, who provided enough information to cause considerable damage to the Soviet Union, was far more likely to be trusted. Nonetheless, in addition to the fact that classified information was tightly restricted, sometimes leaving agents without means to access information beyond their working purview or to smuggle such information home, the tradecraft available to agents was limited at best. Commercial cameras were typically simpler to use but posed far greater odds of compromising the agent in both the office and home environment. Concealed miniature cameras were far more secure, but their awkward operability required delicate handling, constraining their use in occupied spaces while pushing up the need for confidence in the agent. As such, the best tools for the job were largely reserved to a handful of agents who were sufficiently trusted and tested, thereby restricting their outreach.

Although counterintelligence reduced the opportunities available to intelligence officers and their sources, it is clear that human behaviour influenced the final outcome. Given that technology is shaped by the limitations of science, intelligence officers were able to make sound judgements as to how certain tools might function. However, human behaviour proved far more difficult to predict. Some technologies were operationally ill-fitting due to calculable risks, but even when innovation offered evident opportunities, we see a pattern of human behaviour, on the part of the agent or source, negating its potential. In some cases, agents simply rejected technology outright, meaning highly incriminating tools could be introduced that carried little operational value. Moreover, even valued technology was of little benefit if the source or agent could not be trusted to handle it safely or their behaviour was likely to negate its benefits. But in order to understand whether the source or agent exhibited the

personality traits and behaviour required for tradecraft to succeed, intelligence officers needed to develop trust, a factor that rose pursuant to the potential risks at play. And yet, since trust was exceedingly difficult to develop in Moscow's heavily surveilled conditions, tradecraft was either reserved, or applied with an unreasonable chance of failure. Thus, it can be hypothesized that:

- Justifying and mitigating the risks of tradecraft (and technology) in hard target conditions requires greater trust in the behaviour of the prospective or serving spy. Yet, in such conditions the odds of failure are vastly increased since intelligence officers are less able to meet their sources and agents and have less influence over, and insight into, their behaviour.

This is not to say that if human behaviour were addressed, the risks would immediately disappear. Mistakes can happen, counterintelligence can get lucky, and some methods will be just too dangerous to justify regardless. The point is that without addressing human behaviour, difficult situations become far worse, vastly increasing undesirable outcomes. In keeping with the limitations of abduction, it is important to note that this hypothesis requires key assumptions. Espionage will inevitably fail if intelligence agencies do not invest in the training, resources, and personnel required to exploit technology, and it will inevitably succeed if counterintelligence fails to adapt. But assuming that both sides seek to make the most of the opportunities at their disposal, then the end result leans towards human behaviour dictating the final outcome. In hard target conditions, where personal meetings are likely to be at their most insecure, and counterintelligence at its most alert, the end result is weighted towards a pessimistic outcome. Nonetheless, this offers a guiding lesson, or speculative hypothesis, for assessing the strengths and limitations of cyber-enable tradecraft.

Chapter 5
Cyber-enabled recruitment & surveillance

Introduction

In the previous chapter, it was shown that under hard target conditions, the success or failure of tradecraft is increasingly determined by human behaviour, leading towards pessimistic outcomes when behaviour is difficult to predict or control. In this chapter, this hypothesis is tested against cyber developments that are most relevant to *recruitment* and *surveillance.* It builds on the assumptions presented in the literature review, focusing on logical cyber developments that are likely to be of most relevance to their respective functions. The first section thus explores online social communications as a potential means to cultivate and acquire spies, as well as the possibilities of sources volunteering their services by cyber means. The second stage focuses on surveillance, exploring methods of gathering personal information in cyberspace to improve the efficiency of recruitment.

In recruitment, the lens is narrowed to the prospects of using socially innocuous communication systems such as instant messaging, email, and social media, as a means to develop rapport with prospective spies, alongside the possibility of volunteers using intelligence agency websites to pitch their services directly. Its main theme is that through extensive and evolving legislation backed by sweeping technical eavesdropping systems, Internet and telecommunication companies, including mainstream social platforms, are increasingly vulnerable to state surveillance. Its aim, therefore, is to show how Internet surveillance threats are expanding, as the avenues of online social interaction are absorbed into further levels of repressive government controls, with implications both for the cultivation of potential spies and for those who seek to volunteer their services. Consequently, it shows that the levels of risk involved

in overt communication with Russian and Chinese citizens (especially those who live within their domestic borders) are profound, which in turn pushes up the need for trust in the sensibilities of those who are being recruited.

In surveillance, it is argued that open sources and hacking offer the most efficient pathways to personal information. Herein it will be shown that through tight controls over online expression, and the prioritisation of cybersecurity, Russia and China have raised the levels of risk associated with surveillance. While the monitoring of social network accounts or the infection of systems and devices with malicious software (malware), can theoretically provide access to huge sums of personal data, including information which could help to identify and recruit prospective spies, the benefits achieved through online surveillance, whether by open sources or hacking, are tied with rising dangers. This, in turn, increases the need for trust that a target will say or share information that merits the increasing risks.

Recruitment

It is important to reiterate the point that if a target is recruited, or cultivated, from the ground up, then it is crucial for the recruiter to conceal their intentions. If they expose their intelligence affiliations, they risk alarming the target in the early stages of a relationship, who may then end the connection or report their concerns to the security services. The second important factor to note is that as this relationship develops, it is highly likely that two sides will at least occasionally need to meet in person.[1] Given the fact that Russian and Chinese citizens, as members of authoritarian regimes, face dire consequences for aiding foreign powers, the decision to engage in espionage is not an

[1] Gioe, D. V. 'The more things change': HUMINT in the cyber age', in *The Palgrave Handbook of Security, Risk and Intelligence*, edited by Robert Dover, Huw Dylan, and Michael Goodman (London, Palgrave, Macmillan, 2017), p. 221-222.

easy one. According to one former intelligence officer, it has become all the more difficult under the Trump administration, whose apparent fondness for Putin has likely soured the willingness of ideologically motivated Russians to spy for the US government.[2] Steering guarded foreign officials toward an amenable mindset will thus remain a delicate process, while the threat of double agents and dangles will remains an enduring threat, as such face-to-face trust will, in most cases, remain an important bond.[3] But that does not mean that alternative social communications cannot be used to arrange meetings and sustain relationships. While the telephone is still inherently insecure, social communications through the Internet have been proposed as a new, and supposedly secure medium for agent cultivation.[4]

Through a growing myriad of social communications, it seems possible for sources to be cultivated online without, as Wallace argues, 'revealing the hand of an intelligence service'.[5] Similar sentiments are echoed by Tal and Siman-Tov, who purport that through services such as email or social media, sources can be cultivated 'with relatively little risk, at almost no cost, and with almost no effort.'[6] Security of social communications, which by nature are not necessarily covert, rests on the premise that cyberspace is drowning in data, meaning incriminating online activities are less likely to be noticed.[7] As former GCHQ chief David Omand argues, even the largest technical agencies cannot watch everything:

---

[2] Couceiro, C. (March 2017) How the CIA forgot the art of spying, *Politico.* Available at: https://www.politico.com/magazine/story/2017/03/cia-art-spying-espionage-spies-military-terrorism-214875 [accessed 20 January 2018].
[3] Gioe, D. V. 'The more things change', p. 221-222.
[4] See literature review.
[5] Wallace, R. 'A time for counterespionage', in *Vaults, Mirrors, & Masks: Rediscovering U.S. Counterintelligence,* (Washington, Georgetown University Press, 2008), p. 113.
[6] Tal, A. & Siman-Tov, D. 'HUMINT in the cybernetic era: gaming in two worlds', *Military and Strategic Affairs,* 7:3, 2015, p. 97.
[7] In fact, according to Google's former CEO Eric Schmidt, by 2010 worldwide society generated as much information every two days as the rest of recorded history combined through to 2003. For more details, see Tech Crunch (5 August 2010) Eric Schmidt: every 2 days we create as much information as

> The huge growth in the volume of data carried by global communications networks reduces the probability of interception of any given email, text or other message and packet switching means that only parts of a message may be recovered. Microsoft has over a billion users of its Cloud services with 1.3 billion email addresses sending four billion emails a day and uploading 1.5 billion photographs a month. Skype calls via the Internet are taking up two billion minutes per day.[8]

The scope of such data, and its impact on technical intelligence services cannot be understated. As emphasised in a document released by Edward Snowden, NSA (at the time) touched around 1.6 percent 'of total Internet traffic', and yet only 0.025 percent was actually reviewed.[9] As Omand adds, 'the net effect is that NSA analysts look at 0.00004 percent of the world's traffic in conducting their mission'.[10] Yet this American experience is mirrored at a global level, since even in countries where 'massive government surveillance is widespread, the analysis of mass data can be overwhelming'.[11] In short, the information flowing through cyberspace outpaces every nation in the world, creating a morass of ostensibly ordinary noise for conspirators to exploit. This has allowed a plethora of malicious actors, including terrorists, hackers, extremists, criminals and even intelligence officers, to exploit and hide social communications in a growing 'haystack' of data.[12]

The evidence clearly shows that foreign intelligence officers, particularly from Russia and China, are routinely cultivating Western targets through online social platforms.[13] In 2017, the German federal security service, the BfV, accused Chinese

---

we did up to 2003. Available at: https://techcrunch.com/2010/08/04/schmidt-data/ [accessed 16 March 2019]; Ibid.

[8] Omand, D. 'Understanding digital intelligence and the norms that might govern it', *Global Commission on Internet Governance*, 8, 2015, p. 3.

[9] Ibid.

[10] Ibid.

[11] Shavers, B. & Bair, J. *Hiding behind the keyboard: uncovering covert communication method with forensic analysis*, [Kindle version] (Cambridge MA, Syngress, 2016). Accessed 13 August 2017, p. 7.

[12] Runciman, B. 'A bigger haystack…', *ITNow*, 54:2, 2012, p. 36-37.

[13] Reuters (31 August 2018) Exclusive: U.S. accuses China of 'super aggressive' spy campaign on LinkedIn. Available at: https://www.reuters.com/article/us-linkedin-china-espionage-exclusive/exclusive-u-s-accuses-china-of-super-aggressive-spy-campaign-on-linkedin-idUSKCN1LG15Y [accessed 23 October 2018]; Stein, J. (3 August 2017) How Russia is using LinkedIn

operatives of targeting over 10,000 German citizens through professional and social networks such as LinkedIn.[14] As *Newsweek* reported, Chinese intelligence officers were posing as 'academics, business consultants and policy experts', to cultivate relations with 'high profile politicians and business leaders.'[15] But these complaints mirror a far bigger picture, as LinkedIn continues to devolve into a battleground between Russian and Chinese operatives, and opposing Western security services.[16] The problem, as a BfV spokesperson acknowledged, is that any connections to these services are inherently inconspicuous, making it difficult to detect malicious activities unless investigators know where to look.[17] However, one leaked report released by Snowden shows that the West is as equally prepared to cultivate targets through online channels. Written by psychologist Mandeep K. Dhami for GCHQ's *Joint Threat Intelligence Group* (JTRIG), the report reveals how GCHQ officers use cyberspace to 'discredit, disrupt, delay, deny, degrade, and deter' state and none-state threats.[18] Much of this work seems to be focused on manipulating online content for foreign audiences, but occasionally GCHQ tries to cultivate human sources:

> Some of JTRIG's staff have conducted online HUMINT operations. Such operations typically involve establishing an online alias/personality who has a

as a tool of war against its U.S. enemies, *Newsweek.* Available at: https://www.newsweek.com/russia-putin-bots-linkedin-facebook-trump-clinton-kremlin-critics-poison-war-645696 [accessed 23 October 2018]; LinkedIn (10 August 2015) LinkedIn used by Chinese & Russian spies to recruit Brits & steal secrets. Available at: https://www.linkedin.com/pulse/linkedin-used-chinese-russian-spies-recruit-brits-steal-lee-blasdale [accessed 1 January 2018].

[14] Cuthbertson, A. (11 December 2017) China is spying on the west using LinkedIn, intelligence agency claims, *Newsweek.* Available at: http://www.newsweek.com/china-spying-west-using-linkedin-743788 [accessed 1 January 2018].

[15] Ibid.

[16] Manson, K. et al. (30 July 2020) LinkedIn spy scandal shines spotlight on China's online espionage, *Financial Times*. Available at: https://www.ft.com/content/0a0e62a9-65ba-494c-a7bb-86f5f66d627f [accessed 1 December 2020]; Bridge, M. (19 June 2019) Russians created AI redhead on LinkedIn to steal military secrets, *The Times.* Available at: https://www.thetimes.co.uk/article/russians-created-ai-redhead-on-linkedin-to-steal-military-secrets-k2d20lc2z [accessed 1 December 2020]; Wong, E. (27 August 2019) How China uses LinkedIn to recruit spies abroad, *The New York Times.* Available at: https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html [accessed 1 December 2020].

[17] Ibid.

[18] Dhami, M. K. Behavioural science support for JTRIG's (Join Threat Research and Intelligence Group) effects and online HUMINT operations, *Statewatch, GCHQ.* Available at: http://www.statewatch.org/news/2015/jun/behavioural-science-support-for-jtrigs-effects.pdf [accessed 1 January], p. 9-11.

> Facebook page, and membership of relevant web forums, etc. The target is then befriended (or the target befriends the alias). Interactions with the target may be informed by a combination of analysis of SIGINT … monitoring of the target's online behaviour, and intelligence from SIS "on-the-ground". The goal may be to collect intelligence and/or to facilitate SIS contact in order to disrupt, delay, deceive, deter, or dissuade.[19]

In short, GCHQ conducts the groundwork, cultivating online relationships in forums and social networks, before passing the reigns to SIS for the recruitment target to be further developed. However, intelligence officers are not constrained to professional and social networks. In theory, any medium for innocuous social bonding could be harnessed to develop rapport. In stark contrast to the high stakes of espionage, Lucas even suggests that massively multiplayer online games (MMOs) might be a suitable medium to recruit Russian or Chinese officials:

> It would be quite possible to see, for example, who is playing a game from their workplace. If you find that someone whose computer accesses the internet from the Russian defence ministry is a regular player in the small hours, then he is probably some official who is rather bored on his night shifts. With a bit of ingenuity it may be possible find his real-life name. From that the recruiter can start obtaining all the other information: where he lives, what kind of life he leads, how his career is progressing—and what his weaknesses may be.
>
> The recruitment target has no idea of this. What he notices is that he keeps encountering a female protagonist in the game, who sends him friendly, even flirtatious messages. In the heavily male-dominated world of gaming, this is unusual—and potentially welcome news. The friendship deepens, and the Western spy service begins to get into a position where it can make a more substantial approach—perhaps suggesting a meeting "IRL" (in real life). Once that point is reached, the well-honed dark arts of old-style espionage can be applied.[20]

These arguments are hardly baseless, as online video games have proven particularly challenging for state surveillance. Western security services have increasingly struggled to monitor virtual worlds, regarding them as safe havens for terrorists and criminals.[21]

---

[19] Ibid.
[20] Lucas, E. *Spycraft rebooted: how technology is changing espionage,* [Kindle version], (Seattle, Amazon Publishing, 2018), see chapter 6.
[21] Tassi, P. (14 November 2015) How ISIS terrorists may have used PlayStation 4 to discuss and plan attacks [updated], *Forbes.* Available at: https://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/#5b4eb7b70554 [accessed 14 March 2019].

This was illustrated in a GCHQ report disclosed by Snowden, which details the agency's efforts to penetrate 'massively multiplayer online' video games such as, World of Warcraft.[22] This particular massively multiplayer game, known as 'WoW', has attracted over one-hundred million players in its sixteen years of existence.[23] The issue for surveillance, as the report explains, is that communications between players occur over a variety of verbal and non-verbal channels, allowing users to hide their messages 'in plain sight'. [24] For example, if GCHQ is monitoring in-game text chat between players, but not their audio conversations over the popular gaming interface *Discord,* then they may miss vital pieces of evidence.

Moreover, as anthropologist Bonnie Nardi writes, massively online worlds are 'an exemplar of a new means of forming and sustaining human relationships and collaborations through digital technology'.[25] And according to notes from GCHQ's "Network gaming exploitation team", the agency has identified a broad range of potential recruitment targets inside World of Warcraft, including engineers, scientists, embassy chauffeurs, and foreign intelligence officers.[26] As such, just as terrorists use online worlds to conduct what Omand calls 'virtual "meetings", intelligence officers can theoretically mimic this behaviour to securely develop rapport with potential

[22] Snowden Archive (9 December 2013) Exploiting Terrorist Use of Games & Virtual Environments. Available at: https://cryptome.org/2013/12/nsa-gchq-spy-games.pdf [accessed 1 January 2018], p. 7-11.
[23] Blizzard reaches 100M lifetime World of Warcraft accounts (28 January 2014) Polygon. Available at: https://www.polygon.com/2014/1/28/5354856/world-of-warcraft-100m-accounts-lifetime [accessed 20 March 2020].
[24] Snowden Archive (9 December 2013) Exploiting Terrorist Use of Games & Virtual Environments. Available at: https://cryptome.org/2013/12/nsa-gchq-spy-games.pdf [accessed 1 January 2018], p. 8.
[25] Nardi, B. *My life as a Night Elf Priest: An Anthropological Account of World of Warcraft,* (Ann Arbor, The University of Michigan Press, 2010), p 5.
[26] Mazetti, M. & Elliott, J. (10 December 2013) Spies infiltrate a fantasy realm of online games, *The New York Times.* Available at: http://www.nytimes.com/2013/12/10/world/spies-dragnet-reaches-a-playing-field-of-elves-and-trolls.html?mtrref=onlinelibrary.wiley.com&gwh=EE5694212E9FCD4467863E62E311F74E&gwt=pay [accessed 1 January 2018].

sources inside foreign governments.[27] According to reports, the FBI, CIA, and various intelligence agencies are running HUMINT in online games, including the popular online world *Second Life,* to such extent that they even had to establish a "deconfliction" group to avoid overlapping operations.[28]

Another important aspect to consider is the proliferation of social encryption. In 1991, Phil Zimmerman transformed online security when he publicly released the source code for his asymmetric encryption system, *Pretty Good Privacy* (PGP).[29] Whereas conventional symmetric models required the receiver of a message to know the sender's cipher key, asymmetric models, using an elaborate mathematical formula, allowing two people who had never met in person (and therefore never exchanged keys) to share encrypted messages.[30] As Aldrich explains:

> The sender, who we will call 'Alice', secures her message to her friend 'Bob' with a cypher that works like a padlock to which Bob does not have the key. When Bob receives it, instead of trying to open it, he adds a second padlock that depends on a cypher of his own devising, and sends it back to Alice. Alice then removes only her original padlock and sends it back to Bob, by which time it is only secured by Bob's padlock. Bob can now open the box and read the message. They have communicated securely, yet there has been no key distribution.[31]

PGP's release was near revolutionary, offering the first secure means of communication between strangers in cyberspace. Yet, while the strength of its encryption created concerns for agencies such as GCHQ, PGP was notoriously difficult to use, curtailing its wider popularity.[32] But Snowden's surveillance disclosures further transformed

---

[27] Omand, D. 'Understanding digital intelligence', p. 3; Stevens, T. 'Security and Surveillance in Virtual Worlds: Who Is Watching the Warlocks and Why?, *International Political Sociology*, 9, 2015, pp. 231; Lucas, E. *Spycraft rebooted*, see chapter 6.
[28] Snowden Archive (9 December 2013) Exploiting Terrorist Use of Games & Virtual Environments. Available at: https://cryptome.org/2013/12/nsa-gchq-spy-games.pdf [accessed 1 January 2018], p. 10.
[29] Bartlett, J. *The dark net: inside the digital underworld*, (London, William Heinemann, 2014), p. 80
[30] Aldrich, R. J. *GCHQ: the uncensored story of Britain's most secret intelligence agency* [Kindle version] (London, HarperPress, 2010). Accessed 21 January 2021, p. 489-490.
[31] Aldrich, R. J. *GCHQ*, p. 489-490.
[32] Ibid, p. 491-492; Bartlett, J. *The dark net*, p. 80-81; Katwala, A. (17 May 2018) We're calling it: PGP is dead, *Wired*. Available at: https://www.wired.co.uk/article/efail-pgp-vulnerability-outlook-thunderbird-smime [accessed 20 March 2020].

social communication privacy, by encouraging mainstream Internet companies to automate the encryption process.[33] As argued by James Clapper, the former US Director of National Intelligence, "[as] a result of the Snowden revelations, the onset of commercial encryption has accelerated by seven years".[34] In 2016, *WhatsApp* made end-to-end encryption (another term for asymmetric encryption, but more strongly associated with instant messaging) the default setting for one and a half billion users.[35] Similarly, Apple's *iMessenger* offers default encryption to another billion global users, while many other services, such as Russia's *Telegram,* offer opt-in encryption to hundreds of millions of users.[36] Thus, relatively strong, free-to-use encryption shifted from the sole domain of a handful of technically proficient privacy enthusiasts, towards something of a social communication norm.

Even if these companies wanted to cooperate with law enforcement, only their customers' devices actually know the corresponding cipher keys. Consequently, authorities are increasingly struggling to retrieve communication logs from key services (particularly Whatsapp) even after major incidents.[37] This makes these services appetising tools for privacy activists and malicious actors alike, as echoed by Clapper,

[33] The Intercept (25 April 2016) Spy chief complains that Edward Snowden sped up spread of encryption by 7 years. Available at: https://theintercept.com/2016/04/25/spy-chief-complains-that-edward-snowden-sped-up-spread-of-encryption-by-7-years/ [accessed 23 May 2020]
[34] Ibid.
[35] Burgess, M. (9 May 2017) WhatsApp now encrypts iCloud back-ups of your conversations, *Wired*. Available at: http://www.wired.co.uk/article/WhatsApp-encryption-end-to-end-turned-on [accessed 1 March 2018].
[36] Reisinger, D. (6 March 2017) Here's how many iPhones are currently being used worldwide, *Fortune*. Available at: http://fortune.com/2017/03/06/apple-iphone-use-worldwide/ [accessed 1 March 2018]; Greenberg, A. (4 October 2016) You can all finally encrypt Facebook messenger, so do it, *Wired*. Available at: https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/ [accessed 11 January 2018]; The Verge (11 January 2018) Skype starts testing new 'private conversations' with end-to-end encryption. Available at: https://www.theverge.com/2018/1/11/16878596/microsoft-skype-end-to-end-encryption-private-conversations [accessed 5 February 2018]; Tech Crunch (27 October 2013) Meet Telegram, a secure messaging app from the founders of VK, Russia's largest social network. Available at: https://techcrunch.com/2013/10/27/meet-telegram-a-secure-messaging-app-from-the-founders-of-vk-russias-largest-social-network/ [accessed 5 February 2018].
[37] BBC News (27 March 2017) WhatsApp's privacy protections questioned after terror attack. Available at: https://www.bbc.co.uk/news/technology-39405178 [accessed 12 May 2020].

who claimed that the post-Snowden encryption boom had "a profound effect on our ability to collect, particularly against terrorists".[38] His points were further underscored when Facebook revealed its new encrypted chatting service, known as 'Secret Conversations'¸ which was denounced by some politicians as the "service of choice" for terrorists.[39] Furthermore, brute force decryption is unlikely to pose much threat, since most messaging services use a highly regarded cipher system known as AES-256; at current computational levels, this cipher would require the most advanced supercomputers in the world around a billion years to break.[40] But as with video games, what may be advantageous for terrorists and criminals can also prove useful for intelligence officers. In theory, end-to-end encryption could bring some of the benefits of covert communication to the recruitment stage.

Hence, from one perspective, cyberspace appears to offer the ideal conditions for building secure relationships with potential sources. However, while the Western world, whose security services are often constrained by concerns of proportionality and civil liberty, has struggled to keep up with the scale and complexities of online social communications, authoritarian regimes do not necessarily share the same constraints. At the very minimum, Snowden's disclosures revealed that despite the amount of noise generated in cyberspace, governments had still managed to filter through extremely large volumes of traffic.[41] They also carried an ironic consequence, by giving

[38] The Intercept (25 April 2016) Spy chief complains that Edward Snowden sped up spread of encryption by 7 years. Available at: https://theintercept.com/2016/04/25/spy-chief-complains-that-edward-snowden-sped-up-spread-of-encryption-by-7-years/ [accessed 23 May 2020]
[39] Gaines, L. K. & Miller, R. L. *Criminal justice in action: 10th edition,* (Boston, CENGAGE, 2019), p. 551.
[40] IBM Knowledge Center – National Security Agency (NSA) Suit B cryptography. Available at: https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy11025_.htm [accessed 1 July 2018]; Schneier, B. *Data and Goliath: the hidden battles to collect your data and control your world,* [Kindle version] (New York, W. W. Norton & Company, 2015), p. 143.
[41] Brown, I. & Korff, D. 'Foreign surveillance: law and practice in a global digital environment', *European human rights law review*, 2014, 3, p. 2.

dictatorships the ideal leverage to enact draconian data laws.[42] Using the threat of US Internet surveillance as justification for their actions, numerous regimes, including Russia and China, have forced companies to store their data within domestic servers, undermining foreign eavesdropping while shoring up their own surveillance powers. As a consequence, despite citing civil liberty as the rationale for his disclosures, Snowden's actions have increased the threat of surveillance in regimes who have little regard for it.[43] To fully appreciate why cyberspace would be insecure for agent recruitment, an argument that seems to run contrary to the assumption that tools such as WhatsApp are ideal for malicious actors, it is necessary to examine the Internet surveillance powers developing in Russia and China.

Unlike its Western counterparts, China built its Internet infrastructure from the ground up to cement its authoritarian grip.[44] Facilitated by state owned telecommunications and Internet companies (China Telecom, China Mobile, and China Unicom), the government developed a system of filters and chokepoints dubbed the "Great Firewall"; this is, in essence, a censorship goliath, restricting citizens from accessing or even sharing any information that might provoke the regime's disapproval.[45] The Great Firewall is a powerful tool for silencing political dissent and promoting the state's chosen narrative.[46] To maintain such widespread control, the

[42] Hill, J. F. 'The growth of data localization post-Snowden: analysis and recommendations for U.S. policymakers and business leaders', *The Hague Institute for Global Justice, Conference on the Future of Cyber Governance,* 2014, p. 3-4; Sargsyan, T. 'Data localization and the role of infrastructure for surveillance, privacy, and security', *International Journal of Communication,* 2016, p. 2225-2229; Castro, D. & McQuinn, A. 'Beyond the USA Freedom Act: How U.S. surveillance still subverts U.S. competitiveness', *Information Technology & Innovation Foundation,* 2015, p. 2.
[43] Ibid.
[44] Deibert, R. J. *Black code: inside the battle for cyberspace,* (Toronto, McClellend & Stewart, 2013), p. 62.
[45] Deibert, R. & Rohozinski, R. 'Beyond denial: introducing next-generation information access controls', in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace,* [Kindle version] (London, The MIT Press, 2010). Accessed 20 May 2020, p. 3.
[46] Economy, E. C. (29 Jun 2018) The Great Firewall of China: Xi Jinping's internet shutdown, *The Guardian.* Available at https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown [accessed 12 June 2020]; Inkster, N. *China's Cyber Power*, [Kindle Version] (Abingdon, Routledge, 2016). Accessed 20 May 2017, see chapter 1.

government has long relied on outsourcing much of its surveillance machinery to the private sector, '[contrary] to the principles of network neutrality, ISPs, hosting companies, websites, chat clients, and blogs operating in China are all require to police their networks.'[47] For instance, Microsoft *TOM-Skype* (Skype designed for Chinese users) has developed software to detect and block politically undesirable content, using automated systems known as deep-packet inspection.[48]

By 2010, several Western companies, including Google, Facebook and Twitter, had been blocked for either refusing to comply with, or falling foul, of China's censorship regime.[49] But Snowden's 2013 allegations of US eavesdropping suddenly 'served as a perfect opportunity' for the state to strength its controls over communication data.[50] Through its 2015 Counter Terrorism Law, the government instructed both national and foreign companies to store almost all Chinese user data within the mainland, where, as privacy advocates feared, it could be accessed by the authorities.[51] The law forced companies to provide 'technical support, including backdoor access and decryption' to the state for preventing and investigating terrorist activities.[52] These rules were later strengthened in its 2016 Cybersecurity Law, broadening the banner of 'critical infrastructure' to include Internet sites, services, and telecommunications networks.[53] The law also sets out further rules for 'network operators', a loosely defined term which includes any organisation who operates a

[47] Deibert, R. J. *Black code*, p. 73.
[48] Ibid, p. 119.
[49] Fouberg, E. H. & Murphy, A. B. *Human geography: people, place, and culture*, (Hoboken, Wiley, 2015), p. 110.
[50] Sargsyan, T. 'Data localization and the role of infrastructure for surveillance, privacy, and security', p. 2225-2229
[51] The Diplomat (23 January 2016) China's comprehensive counter-terrorism law. Available at: https://thediplomat.com/2016/01/chinas-comprehensive-counter-terrorism-law/ [accessed 11 January 2018].
[52] Ibid.
[53] Clayton Utz (7 December 2017) Comply or be prepared to pay: China's new cybersecurity law. Available at: https://www.claytonutz.com/knowledge/2017/december/comply-or-be-prepared-to-pay-chinas-new-cybersecurity-law [accessed 1 June 2018].

network, ranging from small businesses to mainstream social media companies.[54] Akin to critical infrastructure, any organisation falling under this umbrella is compelled to store personal data about their customers' within mainland China, including any social communications sent through their services.[55]

These rules have also allowed the government to clamp down on encrypted messaging services, as underscored when after years of tentative restrictions, China fully blocked WhatsApp in 2017, denying access to its services nationwide.[56] As of 2019, Apple is the only company in the country with an end-to-end messenger service which has been approved by the state.[57] However, to comply with the Cybersecurity Law, Apple has relocated all of its iCloud data relating to Chinese users, including its 'Cloud Key Vault' (which includes customers' encryption keys, which even Apple itself cannot theoretically access) to an entirely new data centre being constructed in Guizhou.[58] As cryptographic specialist Matthew Green argues, this raises questions about Apple's capacity to keep its customers' data encrypted, especially given China's apparent lack of tolerance for digital privacy, '[this] means that either *(1)* at least some data *will* be totally inaccessible to the Chinese government, or *(2)* Apple has somehow weakened the version of Cloud Key Vault deployed to Chinese users. The latter …

[54] China Law Translate (11 July 2016) 2016 cybersecurity law. Available at: http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en [accessed 21 January 2018].
[55] Reuters (7 November 2016) China adopts cyber security law in face of overseas opposition. Available at: https://www.reuters.com/article/us-china-parliament-cyber/china-adopts-cyber-security-law-in-face-of-overseas-opposition-idUSKBN132049 [accessed 21 January 2018].
[56] Che, X. & Ip, B. *Social networks in China*, (Cambridge, Massachusetts, Chandos Publishing, 2018), p. 40-41; Bradsher, K. (25 September 2017) China blocks WhatsApp, broadening online censorship, *The New York Times.* Available at: https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html [accessed 3 November 2017].
[57] The Verge (25 October 2018) How China complicates Apple's chest-thumping about privacy. Available at: https://www.theverge.com/2018/10/25/18020508/how-china-complicates-apples-chest-thumping-about-privacy [accessed 21 December 2018].
[58] Quartz (18 May 2016) It's official – China is the largest iPhone market in the world. Available at: https://qz.com/687017/its-official-china-is-the-largest-iphone-market-in-the-world/ [accessed 21 January 2018]; The Verge (13 June 2017) Apple is building its first China-based data center per new cybersecurity law. Available at: https://www.theverge.com/2017/7/13/15964220/apple-china-data-center-icloud-new-cybersecurity-law-guizhou [accessed 24 January 2018].

would raise even deeper questions about the integrity of Apple's systems.'[59] As added by Facebook's former chief security officer, Alex Stamos, there is little reason to assume that Apple will refuse to concede to the Ministry of State Security's demands, since it is legally obliged to cooperate.[60] Even if Apple's iMessage service remains encrypted, the corporation accounts for only a declining 6.7 percent of China's smartphone market, with most Chinese citizens opting for cheaper, less independent, domestic products.[61] Consequently, by absorbing mainstream companies under draconian data laws, China has monopolised its access to social communications, ensuring that data can be accessed at its own discretion.

In contrast, prior to Snowden's disclosures, the Internet in Russia was relatively free and uncensored, a factor that stood in stark contrast to Putin's increasingly powerful security services.[62] But as social communications grew in popularity, senior FSB officials became concerned that the 'uncontrolled use' of foreign services such as 'Skype, Gmail, and Hotmail' would challenge Russia's security, since they utilised servers and encryption that could not 'be easily accessed.'[63] Thus, when Putin labelled cyberspace a "CIA project" in 2014, he stoked fears that the Kremlin was gearing up to distort Snowden's surveillance disclosures into a mandate for expanding the government's Internet controls.[64] Those fears actualised through the introduction of the

[59] Green, M. (16 Jan 2018) Apple in China: Who holds the keys?, *Cryptography Engineering.* Available at: https://blog.cryptographyengineering.com/about-me/ [accessed 21 January 2018].
[60] Ibid.
[61] Rapoza, K. (7 January 2019) In Apple loss, how big a deal is China, really?, *Forbes*. Available at: https://www.forbes.com/sites/kenrapoza/2019/01/07/in-apple-loss-how-big-a-deal-is-china-really/#278a659e1aa1 [accessed 3 February 2019].
[62] Deibert, R. & Rohozinski, R. 'Control and subversion in Russian cyberspace', in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace,* [Kindle version] (London, the MIT Press, 2010). Accessed 13 May 2020. p. 15.
[63] Lowenthal, M. *Intelligence: From secrets to policy,* [Kindle version], (Thousand Oaks, CQ Press, 2017). Accessed 30 February 2017, see chapter 17.
[64] MacAskill, E. (24 April 2014) Putin calls Internet a 'CIA project' renewing fears of web breakup, *The Guardian.* Available at: https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia [accessed 20 August 2016].

2015 Data Localization Act, that set out, purportedly, to protect Russian citizens from the "misuse of their personal data by foreign companies and surveillance by foreign governments."[65] In actuality, the law threatened to block companies from access to Russia's growing online market, unless they agreed to store Russian citizens' data within the mainland, where it could coincidentally be accessed by the FSB. Moreover, because the scope of the law applied to companies who stored names, emails, phone numbers, and social media accounts, mainstream foreign companies including Apple, Facebook and Google, all fell under its umbrella.[66] Hence, Russia became the 'first modern economy to attempt full data localisation', with the Kremlin essentially forcing companies of domestic and foreign origin to submit to the authority of the state at the threat of expulsion from a vibrant Internet market.[67]

Once companies relocated their data to Russia, they fell vulnerable to the FSB's technical eavesdropping system, known as SORM.[68] Practically all major Internet and telecommunication companies with servers in Russia are compelled to install SORM equipment, feeding data, including telephone, email, and social media traffic, directly to FSB facilities.[69] That information can be accessed at the FSB's discretion, without any need to give a warrant to the data operator:

> In most Western nations, law enforcement or intelligence agencies must receive a court order before wiretapping. That warrant is sent to phone operators and Internet providers, which are then required by law to intercept the requested information and forward it to the respective government agencies. In Russia, FSB officers are also required to obtain a court order to eavesdrop, but once they have it, they are not required to present it to anybody except their superiors in the FSB. Telecom providers have no right to demand that the FSB show them the warrant. The providers are required to pay for the SORM equipment and its

[65] Garrie, D. & Byhovsky, I. 'Privacy and data protection in Russia', *Journal of Law and Cyber Warfare,* 5:2, 2017, p. 241-242.
[66] Ibid.
[67] Bauer. et al. 'Data localisation in Russia: A self-imposed sanction', *European Centre for International Political Economy,* 6, 2015, p. 2.
[68] Huffington Post (6 December 2016) Once a defender of Internet freedom, Putin is now bringing China's Great Firewall to Russia. Available at: https://www.huffingtonpost.com/andrei-soldatov/putin-china-internet-firewall-russia_b_9821190.html [accessed 31 January].
[69] Deibert, R. & Rohozinski, R. 'Control and subversion', p. 27.

installation, but they are denied access to the surveillance boxes.[70]

As one anonymous FSB officer told *Wired,* they "can use SORM to take stuff off their servers behind their backs"[71] The point, is that the data localization law placed foreign 'Internet giants' on the same footing as domestic providers, obligating them to expose their customers' data with no 'way to know what is intercepted by SORM'.[72] Attempts to resist these measures have been met with a severe response. Russia completely blocked access to LinkedIn in 2016 for refusing to comply with the new regulations, while further threats have allegedly resulted in the compliance of Google, Apple, Facebook, and other mainstream corporations.[73]

The Kremlin has also taken steps to delegitimise social encryption, through a 2016 bill dubbed Yarovaya's law.[74] The law obligates telecommunications and Internet providers to store the content (for six months) and metadata (for three years) of every mobile call, text message, and Internet communication in Russia, in a move since criticised for its unrealistic financial cost.[75] But, it also demanded that all Russian data

[70] Soldatov, A. & Borogan, I. 'Russia's surveillance state', *World Policy Journal,* 30:3, 2013, p. 24-25.
[71] Soldatov, A. & Borogan, I. (21 December 2012) In ex-Soviet states, Russian spy tech still watches you, *Wired*. Available at: https://www.wired.com/2012/12/russias-hand/ [accessed 24 January 2018].
[72] Huffington Post (6 December 2016) Once a defender of Internet freedom, Putin is now bringing China's Great Firewall to Russia. Available at: https://www.huffingtonpost.com/andrei-soldatov/putin-china-internet-firewall-russia_b_9821190.html [accessed 31 January].
[73] Tech Crunch (17 November 2017) LinkedIn is now officially blocked in Russia. Available at: https://techcrunch.com/2016/11/17/linkedin-is-now-officially-blocked-in-russia/ [accessed 31 January 2018]; Tech Crunch (7 March 2017) Russia says 'nyet,', continues LinkedIn block after it refuses to store data in Russia. Available at: https://techcrunch.com/2017/03/07/russia-says-nyet-continues-linkedin-block-after-it-refuses-to-store-data-in-russia/ [accessed 31 January 2018]; Datacenter Dynamics (14 September 2015) Russian data law: Apple complies, Google and Facebook delay. Available at: http://www.datacenterdynamics.com/content-tracks/design-build/russian-data-law-apple-complies-google-and-facebook-delay/94785.fullarticle [accessed 31 January 2018]; The Telegraph (27 September 2017) Russia threatens to ban Facebook in election year. Available at: http://www.telegraph.co.uk/news/2017/09/27/russia-threatens-ban-facebook-election-year/ [accessed 31 January 2018].
[74] Luhn, A. (26 June 2016) Russia passes 'Big Brother' anti-terror laws, *The Guardian.* Available at: https://www.theguardian.com/world/2016/jun/26/russia-passes-big-brother-anti-terror-laws [accessed 21 January 2021].
[75] Meduza (24 June 2015) Russia's state Duma just approved some of the most repressive laws in post-Soviet history. Available at: https://meduza.io/en/feature/2016/06/24/russia-s-state-duma-just-approved-some-of-the-most-repressive-laws-in-post-soviet-history [accessed 24 January 2018].

be surrendered to the state upon request.[76] Since end-to-end services cannot provide the cleartext communications of their customers, they are essentially in breach of the rules and, therefore, at risk of being blocked.[77] As a sign of the Kremlin's determination to clamp down on encrypted providers, in 2018 the government attempted to block access to the encrypted messenger *Telegram,* after the company refused to modify its software or make concessions to the Kremlin's demands.[78] Given that Telegram is one of Russia's most popular encrypted platforms, especially amongst more affluent circles and the political elite, its ban can be interpreted as a warning to rival companies.[79] As one government official asserted, if other services, such as WhatsApp, fail to comply with Yarovaya's Law, they too "will be blocked sooner or later".[80] Nevertheless, this show of strength was severely undermined when the government inadvertently blocked millions of Amazon and Google services who's servers Telegram had used to piggyback its own systems (in short, the FSB was unable to differentiate Telegram services from Amazon or Google's, thereby blocking everything in the process).[81] To this day, Russia has still not been able to fully block access to Telegram's dispersed IP

[76] Electronic Frontier Foundation (19 July 2016) Russia asks for the impossible with its new surveillance laws. Available at: https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws [accessed 21 July 2020].
[77] Human Rights Watch (18 June 2020) Russia: growing internet isolation, control, censorship. Available at: https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship [accessed 10 September 2020].
[78] Roth, A. (13 April 2018) Moscow court bans Telegram messaging app, *The Guardian.* Available at: https://www.theguardian.com/world/2018/apr/13/moscow-court-bans-telegram-messaging-app [accessed July 2020].
[79] The Verge (17 April 2018) Russia's Telegram ban is a big, convoluted mess. Available at: https://www.theverge.com/2018/4/17/17246150/telegram-russia-ban [accessed 20 November 2018].
[80] Sudakov, D. (2 May 2017) Russia may block WhatsApp, Viber, Telegram even tomorrow, *Pravda*. Available at: http://www.pravdareport.com/business/companies/02-05-2017/137639-messaging_service_russia-0/ [accessed 31 January 2018].
[81] BBC News (23 April 2018) Russia Telegram ban hits Google and Amazon services. Available at: https://www.bbc.co.uk/news/technology-43865538 [accessed 20 November 2018].

addresses without causing disruptions to other services, exposing the government's strained capacity to follow through on its threats.[82]

Consequently, both regimes have imposed the legal, technical, and political foundations to isolate their citizens from uncooperative services, and, in turn, reinforce their own surveillance powers. In fact, Russia's ability to isolate the entire state within a fully monitored system was demonstrated in December 2019, when the government cut off all access to the outside Internet for a multi-day experiment.[83] While the details of the test were kept vague, it could be argued that, due to data localization, the event was barely noticed by most citizens using local services.[84] Yet, for intelligence officers attempting to recruit their quarry with any semblance of security, these measures severely impede their options. For instance, in comparison to Lucas' suggestion of using video games to recruit hard target sources, even those mediums have been affected by the new rules.[85] The popular online video game, *League of Legends*, has suspended all voice chat functionality for its Russian players, because its developers were otherwise obligated to store that data by Yarovaya's Law.[86] China, meanwhile, is reportedly in the process of banning all interaction and communication with foreigners in online video games, due to what it perceives as a key security loophole.[87] Thereby

[82] Burgess, M. (28 April 2018) This is why Russia's attempts to block Telegram have failed, *Wired*. Available at: https://www.wired.co.uk/article/telegram-in-russia-blocked-web-app-ban-facebook-twitter-google [accessed 20 November 2018].
[83] BBC News (24 December 2019) Russia 'successfully tests' its unplugged internet. Available at: https://www.bbc.co.uk/news/technology-50902496 [accessed 20 March 2020].
[84] Ibid.
[85] Lucas, E. *Spycraft rebooted: how technology is changing espionage*, [Kindle version], (Seattle, Amazon Publishing, 2018). Accessed 5 January 2019, see chapter 6.
[86] Nerd4.life (27 March 2020) Players from Russia will not be able to use voice chat in a shooter Valorant. Available at: https://nerd4.life/2020/03/27/players-from-russia-will-not-be-able-to-use-voice-chat-in-a-shooter-valorant/ [accessed 14 December 2020].
[87] Taiwan News (15 April 2020) China to ban online gaming, chatting with foreigners outside Great Firewall: report. Available at: https://www.taiwannews.com.tw/en/news/3916690 [accessed 9 May 2020].

implying that no social medium is likely to go unscathed, with each new rule further diminishing notions of online privacy.

Consequently, any attempt to cultivate a source in cyberspace risks leaving what Brown and Korff describe as a 'digital scarlet letter'.[88] By expanding their laws, surveillance states can see both the metadata of messages (metadata is essentially data about data, including time, data, location, usernames, IP addresses, services, and devices), alongside the content of those communications.[89] To put these issues in perspective, it is worth drawing comparison to three Russian intelligence officers arrested in the United States in 2015. As explained in the FBI's indictment, Evgeny Buryakov, Igor Sporyshev, and Victor Podobnyy, all sought to avoid incriminating conversations over telephones, email, or any other electronic means, while working in in US territory.[90] However, they did, somewhat contradictorily, contact their target for recruitment (who is identified in the report as Male-1, but is in fact Donald Trumps' former policy advisor, Carter Page) by email.[91] Precisely why this lapse in tradecraft occurred has not been fully explained, but the decision to contact a presidential candidate's advisor by electronic mail ultimately proved a poor one. Data trails allowed the FBI to access several months of email records, turning every communication sent by the trio into evidence to be used against them in court.[92] And while no evidence

[88] Brown, I. & Korff, D. 'Foreign surveillance', p. 246.
[89] Ibid.
[90] United States of America v. Evgeny Buryakov, a/k/a "Zhenya,", Igor Sporyshev, and Victor Podobnyy, *Department of Justice,* 2015, p. 7.
[91] As Gioe notes, it's unclear whether Carter was an intentional or incidental source, nevertheless, he was a valuable asset '[it] seems clear that Carter Page was a naïf in over his head in pursuit of lucrative Russian energy deals. While maintaining he did nothing inappropriate, his role – even if unwitting – in the mosaic of Russian hybrid intelligence was significant and earns him the characterization of useful fool for Russian intelligence'. For more details, see Ibid, p. 13; Harding, L. (3 February 2018) Why Carter Page was worth watching, *Politico.* Available at: https://www.politico.com/magazine/story/2018/02/03/carter-page-nunes-memo-216934 [accessed 24 February 2018]; Gioe, D. V. 'Cyber operations and useful fools: the approach of Russian hybrid intelligence', *Intelligence and National Security,* 33:7, 2018, p. 967.
[92] United States of America -v.- Evgeny Buryakov, p. 13, 19, & 23.

implicated Carter directly, the very existence of the emails by Russian intelligence officers was enough to put the political advisor under intense suspicion.[93]

However, this is not to suggest that cracks in surveillance machinery cannot occur. This too was illustrated in a case reported in Chinese state media involving a low-level agent known as 'Li', who was reportedly recruited and handled through social media by a foreign operative dubbed 'Feige'.[94] In one respect, the fact that Li was supposedly run for several years through China's QQ social network, suggests, as Mattis argues, that despite the government's vast surveillance powers, its security services still have 'trouble tracking the flow of information.'[95] Yet it bears note that once the authorities discovered Feige's accounts, they were able to trace everyone he or she had contacted, unmasking around forty additional sources.[96] The point being, Feige's online activities remained safe only until suspicions were honed, at which point China's surveillance system left the operative's online misdemeanours fully exposed.[97] Hence, although social communication can be hidden in the noise, this offers little assurance. Once counterintelligence knows which accounts to focus on, security services can access data with minor obstruction, whereupon years' worth of incriminating communications may be laid bare.

Thus, for intelligence officers posted in Beijing or Moscow, it would be sensible to assume that their online activity would be monitored around the clock. It is, however, possible that recruiters could pursue targets from the comfort of Langley, operating,

---

[93] Harding, L. (3 February 2018) Why Carter Page was worth watching, *Politico.* Available at: https://www.politico.com/magazine/story/2018/02/03/carter-page-nunes-memo-216934 [accessed 24 February 2018].
[94] Brookes, A. (4 November 2014) Is China swarming with foreign spies?, *Foreign Policy.* Available at: http://foreignpolicy.com/2014/11/04/is-china-swarming-with-foreign-spies/ [accessed 11 January 2018].
[95] The Jamestown Foundation (7 May 2014) Virtual espionage challenges Chinese counterintelligence. Available at: https://jamestown.org/program/virtual-espionage-challenges-chinese-counterintelligence/ [accessed 1 January 2017].
[96] Ibid; Yixue W. (5 September 2014) Guard secrets against spy net, *China Daily.* Available at: http://www.chinadaily.com.cn/opinion/2014-05/09/content_17494978.htm [accessed 12 August 2017].
[97] Ibid.

like Feige, on accounts completely unknown to counterintelligence. Herein, however, there is a growing risk that the targets of recruitment may be under their own surveillance. India reportedly placed over 2,000 serving and former military personnel under surveillance after discovering that Pakistani intelligence officers were recruiting military officials through social media.[98] Similarly, China forced PLA soldiers to install eavesdropping software on personal devices monitored by commanding officers, curbing behaviours that harm the 'political spirit' of the army.[99] The authorities have also indicated, through a national propaganda campaign, that they are monitoring social media and online military forums due to rising activity by foreign operatives.[100] Concurrently, in Russia citizens are placed on SORM watchlists for a variety of indiscretions, including attending anti-regime demonstrations or even expressing support for Putin's opponents on social media.[101] Official figures show that in a mere six years, annual SORM intercepts doubled, rising to 539,864 cases by 2012.[102] Yet, this figure could be far higher, since it does not include the number of targets subjected to SORM surveillance for counterintelligence purposes.[103] Therefore, although foreign officials can be contacted via accounts that are unknown to the opposing side, there is a realistic possibility that the target's social communications, rather than the recruiter's, are already being monitored, if only haphazardly.

[98] Shekhar Shashank (29 December 2015) Security agencies watch 2,000 officers' social media profiles after ISI honey-trap, *Daily Mail India*. Available at: http://www.dailymail.co.uk/indiahome/indianews/article-3378134/Security-agencies-watch-2-000-officers-social-media-profiles-ISI-honey-trap.html [accessed 1 January 2018].
[99] Ge, C. (19 April 2016) PLA on call: China's military orders anti-spy software for soldiers' smartphones, *South China Morning Post.* Available at: https://www.scmp.com/news/china/diplomacy-defence/article/1937085/pla-call-chinas-military-orders-anti-spy-software [accessed 1 January 2018].
[100] Global Times (28 August 2014) Peeking in China: spying targets and tactics. Available at: http://www.globaltimes.cn/content/878779.shtml [accessed 20 March 2016].
[101] Morgus, R. 'The spread of Russia's digital authoritarianism', in *Artificial Intelligence, China, Russia and the global order*, edited by Nicholas D. Wright, [Kindle version] (Maxwell, Air University Press, 2019). Accessed 1 January 2020, p. 90-91.
[102] Soldatov, A. & Borogan, I. 'Russia's surveillance state', p. 25.
[103] Ibid.

Without recourse to privacy, and knowing the odds that they or their targets might already be under some degree of observation, it seems sensible for recruiters to avoid social communications as far as possible.[104] One strong indicator to this effect is the case of Jun Wei Yeo, who served as something of a principal agent for Chinese intelligence.[105] Yeo was a PhD student in Singapore who was tasked by alleged members of a Chinese think tank (who he quickly determined to be Chinese intelligence officers) to collect "political reports and information".[106] When operating *outside* of the US, he was told to communicate by China's encrypted WeChat, changing his account whenever he wanted to communicate with his handlers.[107] But when inside the US, he was firmly told not to take his phone and, if he needed to send an important email, to 'do so from a local coffee shop.'[108] Therefore, when messages were sent that were likely to draw interest from US counterintelligence, namely those to China, total avoidance of social communication was the preferred option, followed by mitigating security steps.[109] However, if these were the precautions given to a low ranking Chinese operative inside of a liberal democracy, it is not difficult to see why intelligence officers trying to recruit spies inside Moscow or Beijing might wish to abstain from social communications completely. Even if a relationship appears to the observer to be purely social, once conversations steer to more sensitive matters, such as the target's feelings on the ruling regime or the types of information they work with, there is a risk that the authorities will intervene.

[104] Email correspondence with David Gioe, by Kyle Cunliffe, 2018
[105] BBC News (26 July 2020) How a Chinese agent used LinkedIn to hunt for targets. Available at: https://www.bbc.co.uk/news/world-asia-53544505 [accessed 12 August 2020].
[106] Ibid.
[107] United States of America v. Jun Wei Yeo, also known as Dickson Yeo, *United States District Court for the District of Columbia,* 2020, p. 6.
[108] Ibid.
[109] Ibid.

But whether recruiters want to avoid social communication or attempt to use it in the most secure fashion possible, they inevitably require trust in their target. At minimum, instructing targets to take precautions similar to Yeo's requires a high degree of trust, since doing so could raise alarms or encourage concerned sources to report suspicious requests to the authorities. Business professionals have justifiable reason to request secure communications from their contacts (e.g. to protect intellectual property), and intelligence officers could use this to their advantage.[110] But when it comes to more social relationships, there are few easy ways to ask a foreign acquaintance to take security precautions, meaning security may be dependent on the other person – the target – taking some form of initiative. Fortunately, in China, self-censorship is extremely common, illustrated by cat-and-mouse games emerging between online citizens and Chinese censors, with the former adopting codewords and metaphors as substitutes for banned and politically sensitive words.[111] When online communities began using pictures of Winnie the Pooh to mock President Xi, the Pooh bear himself became a target of censorship, leading to a ban of the 2018 film, *Christopher Robin*.[112] This tendency toward self-censorship is intentional, with the state's surveillance panopticon allowing citizens to 'publicly vent their spleen against officialdom', while 'remaining uncertain whether a government red line has been crossed, inviting official retribution'.[113] The Chinese government has also not shied away from making its online security concerns clear, as underscored by national

[110] University of Delaware (21 September 2012) Human Intelligence in the digital age: global agenda 2012, *Youtube*. Available at: https://www.youtube.com/watch?v=bfIxarRLMDo [accessed 23 January 2016].
[111] Deibert, R. J. *Black code*, p. 74; Ekman, A. 'China's adaptive Internet management strategy after the emergence of social networks', in *Chinese Cybersecurity and Defense*, edited by Daniel Ventre (London, ISTE, 2014), p. 83.
[112] Haas, B. (7 August 2018) China bans Winnie the Pooh film after comparisons to President Xi, *The Guardian.* Available at: https://www.theguardian.com/world/2018/aug/07/china-bans-winnie-the-pooh-film-to-stop-comparisons-to-president-xi [accessed 13 June 2020].
[113] Inkster, N. *China's Cyber Power,* see chapter 1.

propaganda cartoons warning about the dangers of duplicitous foreign operatives trying to cultivate and entrap Chinese citizens online.[114] These include encouraging vigilance within the family unit, and even amongst children, towards spotting relatives who are being cultivated by mysterious Internet acquaintances.[115] It can thus be assumed that Chinese citizens – especially those with access to secret or sensitive information - are likely to be aware about the precariousness of their online relationships, especially with foreigners, and may be further inclined towards more discreet behaviour, avoiding discussions that may draw the attention of state surveillance.

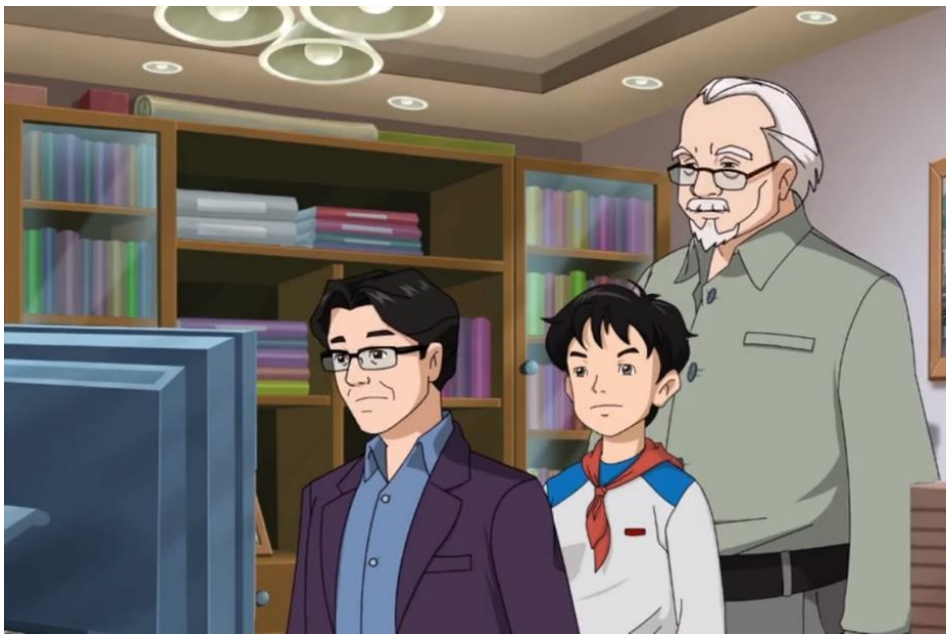

Figure 3: Screenshot from a Chinese 'counterespionage' propaganda cartoon.[116]

[114] The Verge (7 November 2017) China's education group released a cartoon encouraging kids to embrace counterespionage. Available at: https://www.theverge.com/2017/11/7/16617494/china-national-security-spying-propaganda-cartoon-education [accessed 15 January 2021].
[115] K Zhou, V. (6 November 2017) 'Grandpa, what are spies?' Cartoon urges Chinese children to be on alert: National Security Law requires national security to be part of children's education, *South China Morning Post*. Available at: https://www.scmp.com/news/china/policies-politics/article/2118553/grandpa-what-are-spies-cartoon-urges-chinese-children [accessed 16 December 2017].
[116] The Verge (7 November 2017) China's education group released a cartoon encouraging kids to embrace counterespionage. Available at: https://www.theverge.com/2017/11/7/16617494/china-national-security-spying-propaganda-cartoon-education [accessed 15 January 2021].

In Russia, anti-regime protesters long preferred to use Facebook for political mobilisation rather than the Russian social network, Vkontakte (VK) [117] This preference rested on security, as unlike Vkontakte, which is domestically far more popular, Facebook's servers were initially located outside of Russia, beyond the jurisdiction of the FSB.[118] Furthermore, Telegram, which the government has repeatedly attempted to ban, is highly popular among niche areas of society who are interested in political affairs, precisely because its encryption allows sensitive discussions to be made freely.[119] Allegedly, to circumvent restrictions, younger Russians are trying to access Telegram by using anonymising tools such as VPNs (which are discussed in the proceeding chapter), allowing them to gossip on Russian political affairs without interference.[120] And while Facebook may have acquiesced to the Kremlin's data localisation laws, and Telegrams is still being targeted by the FSB, these measures demonstrate that the ingrained Soviet adage "this is not a phone conversation" is still relevant among Russia's online communities.[121] Moreover, according to Judah, self-censorship is even more acute among Russia's elite, who are fearful of being targeted in the next 'wave of sackings, arrests or even purges'.[122] Those 'privy to sensitive information no longer carry smartphones', and instead resort to 'simple old cell phones

[117] Gainous, J. et al, 'Digital media and political opposition in authoritarian systems: Russia's 2011 and 2016 Duma election', *Democratization,* 25:2, 2016, p. 211.
[118] Ibid.
[119] The Verge (17 April 2018) Russia's Telegram ban is a big, convoluted mess. Available at: https://www.theverge.com/2018/4/17/17246150/telegram-russia-ban [accessed 20 November 2018].
[120] Ibid.
[121] As Morgus notes, Russia's entire Internet surveillance strategy rests on self-censorship, through a combination of technical monitoring and oppressive freedom of speech laws. Russia has outlawed 'extreme speech' online, but it's definition of 'extreme speech' has 'been selectively cast … to include relatively benign criticism of the government'. Arguably, any government official, military officer, or nuclear scientist known to have expressed 'benign' criticism of the state, past or present, could quickly find themselves subject to online surveillance. For more details, see
Morgus, R. 'The spread of Russia's digital authoritarianism', p. 90-91.
[122] Judah, B. (19 October 2014) Putin's coup: How the Russian leader used the Ukraine crisis to consolidate his dictatorship, *Politico*. Available at: https://www.politico.com/magazine/story/2014/10/vladimir-putins-coup-112025_full.html#.WJo84H9yXE9 [accessed 1 March 2018].

and now remove the battery – to make sure the phone is dead – when they talk about Kremlin politics among themselves', steps taken out of fear that the FSB might be listening in on their electronic devices.[123] This is naturally a poor reflection on the state of online freedom, but it again increases the probability that recruitment targets will understand, without instruction, the need for discretion. Nonetheless, in Moscow or Beijing conditions, intelligence officers will likely require at least some confidence before sharing their social communication details.

A slow and insecure cultivation process could, however, be avoided altogether if prospective spies can find a secure means to volunteer their services. While entering or phoning foreign embassies, or even approaching foreign officials, remains hazardous for Moscow or Beijing residents, it is possible for candidates to volunteer their services online.[124] Both SIS and the CIA provide online contact forms on their home websites, allowing interested parties to deliver their pitch directly to intelligence agencies.[125] As the CIA website explains, sources can use this system if they want to share information that may be useful to the CIA's 'foreign intelligence mission.'[126] But as SIS's website warns, this approach is exceedingly dangerous, since connections to these websites are likely to be under surveillance:

> Before filling out this form, you should take some sensible precautions. We want to keep you safe and ensure that your contact with SIS is secure. Internet traffic is monitored by most governments. It is also possible, in some circumstances, for specialists to retrieve internet traffic from a device that you have used.
>
> To use this site safely, you should be confident in using the internet in a secure way and have a good understanding of the vulnerabilities of the device and internet connection you are using …

[123] Ibid.
[124] Althoff, M. 'Human intelligence', in *The five disciplines of intelligence collection*, edited by Mark M. Lowenthal &Robert M. Clark (Thousand Oaks, CQ Press, 2016), p. 75.
[125] SIS – Contact us. Available at: https://www.sis.gov.uk/contact-us-form.html?lan=en [accessed 20 September 2017].
[126] CIA - Contact CIA. Available at: https://www.cia.gov/cgi-bin/forlang_form.cgi [accessed 15 September 2020].

> … If possible, do not contact us from inside your own country, or from a country likely to share security information with your country.
>
> … If you are unsure about any of the above, or believe that your contact with SIS through the internet could be intercepted and therefore cause you difficulties, please consider other options such as visiting a British Embassy in person, ideally in a country which has friendly relations with the UK.[127]

This method thus seems no more secure than telephoning an embassy; a source who connects to these services from their phone or home computer could draw the attention of counterintelligence. It is, however, worth noting that Langley has created an official website in the dark web, with the intent to ensure that "individuals can access us securely from anywhere".[128] This might provide at least some level of security for anyone trained in the more nuanced aspects of communication security, such as professional intelligence officers or government hackers, but as the proceeding chapter shows, the tools that enable access to these spaces (namely a programme known as The Onion Router, or Tor) are not necessarily secure.[129]

Owing to these risks, the need for trust in the volunteer is mounting. At the bare minimum, recruiters will need to know that the volunteer has taken necessary security precautions, such as sending their message from a secure location or even from a different country. Securing a response, however, may be proving more difficult, in part because they are easy targets for counterintelligence danglers. It is relatively easy for security services to create 'fictitious volunteers' online, which can be 'used to occupy an opposing services and thus prevent them from finding or working with legitimate volunteers.'[130] Moreover, as Stein candidly argues: '[only] once in a blue moon does

[127] SIS – Contact us. Available at: https://www.sis.gov.uk/contact-us.html [accessed 20 December 2018].
[128] CIA (7 May 2019) CIA's latest layer: an Onion site. Available at: https://www.cia.gov/news-information/press-releases-statements/2019-press-releases-statements/ciagov-over-tor.html [accessed 15 September 2020].
[129] For more details, see chapter 6, section 'Handling'.
[130] Althoff, M. 'Human intelligence', p. 75.

something interesting turn up in all the messages from wannabe spies, students looking for help with their term papers, critics howling about torture and untold thousands of certifiable nuts who insist they're getting radio messages through their teeth'.[131] In 2016, for example, the FSB told Russian media that it had given warnings to two Russian fraudsters caught emailing fake military secrets to the CIA's website.[132] Langley reportedly "took the bait", and "began to start posing questions, especially about the situation at military sites".[133] In addition to wasting the intelligence officers time and resources, the incident also served as something of a propaganda scoop, with Russian media reporting that "the James Bonds from the depths of Siberia led the CIA agents up the garden path."[134]

These threats only increase the likelihood that a genuine volunteer might be overlooked or ignored. Such issues were exemplified in the 2009 case of Roman Ushakov, of Russia's Interior Ministry (MVD).[135] According to Stein (based on interviews with CIA intelligence officers), Ushakov initiated contact through the agency's public website, becoming 'a kind of spotter for the CIA'.[136] Despite his low-ranking status, Ushakov offered identities for around a dozen FSB officers, alongside insider access to the MVD. Potentially, as former CIA analyst Mark Stout argues, Ushakov could have provided information on Russia's national-police force, including on "Russian politics, corruption, and organized crime – information that could help the united states frame its foreign policy vis-à-vis Russia".[137] He might also have offered

[131] Stein, J. (3 July 2015) The Russian spy who came in through the email, *Newsweek.* Available at: https://www.newsweek.com/russian-spy-through-email-312104 [accessed 10 June 2017].
[132] Business Insider (20 September 2016) Russia busts pair 'trying to sell CIA fake secrets'. Available at: https://www.businessinsider.com/afp-russia-busts-pair-trying-to-sell-cia-fake-secrets-2016-9?r=US&IR=T [accessed 15 September 2020].
[133] Ibid.
[134] Ibid.
[135] Stein, J. (3 July 2015) The Russian spy who came in through the email, *Newsweek.* Available at: https://www.newsweek.com/russian-spy-through-email-312104 [accessed 10 June 2017].
[136] Ibid.
[137] Ibid.

information on MVD forces engaged in campaigns in “Chechnya and other hot-spots”.[138] Despite his eventual capture and trial by Russian authorities (he was allegedly caught when attempting to access a dead drop) the case highlights the complications faced by online volunteers. On the one hand, his pitch was taken seriously, with CIA operatives risking the opportunity to assess him face-to-face, at least in a foreign country. On the other hand, based on the likelihood of surveillance against the CIA’s website, combined with Ushakov’s unusual freedom of foreign travel for an MVD official, former CIA officers question his legitimacy:

> … two former CIA officers with long experience combating Russian intelligence said the case smelled like a classic deception operation run by “the Center,” as Moscow’s spy headquarters is known. "It's difficult to imagine that Ushakov is for real,” said Colin Thompson, who spent much of his career targeted on Soviet Russia. "… the internal directorate of the FSB certainly monitors the CIA website, and the CIA should view any Russian volunteer using that channel as a likely provocation or, if not, a fool who should be ignored….”
>
> “Smells like 'chicken feed' from a dangle,” said another former operative, referring to the ersatz defectors that spy services “dangle” in front of each other. "A low-ranking FSB guy would not likely travel abroad so freely,” he said on condition of anonymity to discuss sensitive trade craft. "Maybe FSB let him travel to establish contact.” And the reason Ushakov gave for volunteering to spy for the U.S.—that he was refused a better job? "A classic tell of a dangle is limited access,” said the former operative. That way, he has a plausible reason for telling the CIA "he can only get certain info, not top secrets.” Perhaps Ushakov was genuine in the beginning, he said, but Russian intelligence almost certainly would have have [sic] noticed his open email to cia.gov and “flipped him."[139]

The words of Colin Thompson here are particularly poignant, that sources who volunteer online are deemed ‘fools’, who are likely to ‘be ignored’. In fact, a lengthy *Meduza* interview with Yevgeny Chistov, a former Russian police officer turned CIA spy (who was sentenced to 13 years for treason), indicates that this problem has

[138] Ibid.
[139] Ibid.

considerably worsened since Ushakov made online contact in 2009.[140] In 2011, Chistov volunteered his services, and while he declines to explain his means of contact (although he notes that he did *not* volunteer through US embassy officials), he acknowledges that his method was relatively simple, taking only ten days. It is speculated that Chistov volunteered his services online, but the report includes one glaring piece of information, 'the CIA now discourages Russians from using that particular means of self-recruitment'.[141] Indeed, for unspecified reasons, the CIA's website now includes the following warning: "Attention: If you are a citizen of the Russian Federation, please do not contact us via this site."[142] In effect, while online volunteering could be secure *if* sources take precautions, it may now prove more difficult for Russian and other hard-target sources to attract Langley's attention. The sources who succeed will likely need to offer a strong case, with evidence of their bona fides and assurances of a secure approach. However, the notion of sending highly incriminating information through a tentatively secure medium is hardly likely to be comforting for would-be spies, and those unprepared to take risks, at least initially, may have little recourse but either luck or persistence.

Surveillance

The burdens of recruitment may be reduced by improving tradecraft for gathering operational data, information that aids in the spotting and assessment of spies. One of the oldest windows into a target's personal affairs, bugging, has been substantially

[140] Meduza (31 July 2019) 'I'd be willing to work against this government with Satan himself' We talked to a suburban Russian policeman who spied for the CIA, fought in eastern Ukraine, and got sentence to 13 years for treason. Available at: https://meduza.io/en/feature/2019/07/31/i-d-be-willing-to-work-against-this-government-with-satan-himself [accessed 15 September 2020].
[141] Ibid.
[142] CIA - Contact CIA. Available at: https://www.cia.gov/cgi-bin/forlang_form.cgi [accessed 15 September 2020].

advanced by microphone and video camera technologies.[143] But the act of invading premises or embassies to plant hidden listening devices is still prohibitively dangerous, especially in hard target conditions. However, it is commonly argued that through new forms of digital surveillance, intelligence officers are able to identify and assess their targets with much greater ease than a classic listening device, '[one] former senior SIS office recalled how, in contrast to the huge efforts and great time once expended to try to find a single Soviet recruit, the key quality of modern espionage was its remarkable speed and efficiency.'[144] With enough information from enough sources, today's intelligence officers may be able to 'rapidly access an unparalleled amount of information about a recruitment target before approaching them', meaning a "pitch" can be 'accelerated' for a greater 'chance of success'.[145]

Although this may be true in most instances, gaining access to vast amounts of personal information pursuant to Russian or Chinese officials is less straightforward. One key avenue to personal data is the mass surveillance practices disclosed by Edward Snowden, not least the vast data-hoarding programme known as PRISM.[146] By legally compelling mainstream Internet companies, including Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, and Apple, to provide backdoors data (thus circumventing encryption) the NSA could read the e-mails, chat records, and online activities of approved targets. All of this was done with the full cooperation of the companies involved, with the data siphoned rather than stolen, through a system of warrants and regulations.[147] Anyone, including Russian or Chinese officials, with an

[143] Wallace, R. et al. *Spycraft: inside the CIA's top secret spy lab,* (London, Bantam Press, 2008), p. 447.
[144] Grey, S. *The new spymasters: inside espionage from the Cold War to global terror,* (New York, Viking, 2015), p. 277.
[145] Ibid.
[146] Greenwald, G. & MacAskill, E. (6 June 2013) NSA Prism program taps in to user data of Apple, Google and others, *The Guardian.* Available at: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Network%20front:network-front%20main-2%20Special%20trail:Network%20front%20-%20special%20trail:Position1 [accessed 19 March 2019].
[147] Ibid.

account in any of these companies could in theory have been targeted, however, owing to the data localisation rules since adopted by these countries, PRISM's utility for espionage is limited.[148] The NSA certainly cannot demand backdoor access to Apple accounts stored in China, nor can it force Facebook to hand over the data it is legally obliged to store in Russian servers.

By contrast, vast amounts of operational data can be harvested through open sources such as social media. For example, an 'astonishing' amount of information is shared on professional networks such as LinkedIn, including employment history, duties, security clearances and other details that could otherwise have taken 'weeks or even months of personal meetings to elicit.'[149] Millions of people often share abundant amounts of seemingly trivial personal details on social networks such as Facebook, including their friends, family, political leanings, hobbies, romantic partners, and even personal crises.[150] Using this information, analysts can potentially determine who has access to sought-after secrets and devise a strategy to recruit them, as former CIA officer Lindsay Moran told *NewsRep*, "[social] networks do a lot of a case officer's work for him or her … So much of a potential target's personal information that used to take months, or even years of rapport, development, and elicitation to uncover, is often right there out in the open.".[151] Armed with this information, astute recruiters can develop a relationship by purportedly sharing the same interests as those disclosed by

[148] Sargsyan, T. 'Data localization', p. 2225-2229
[149] Gioe, D. V. 'The more things change', p. 218.
[150] Such *oversharing* can be tied to a phenomena described by psychologist John Suler as the 'online disinhibition effect', whereby online anonymity (either in terms of a hidden identity or physical invisibility) encourages higher levels of both positive and negative expression. In the cyber world, people often feel more confident to share personal details, hostile or controversial opinions, or to even engage in charitable acts of kindness. For more details, see Suler, J. 'The online disinhibition effect', *Cyberpsychology & Behavior*, 7:3, 2004, p. 321; Lucas, E. *Cyberphobia: Identity, Trust, Security and the Internet*, [Kindle version] (New York, Bloomsbury, 2016). Accessed 1 March 2018, p. 61.
[151] NewsRep (24 March 2015) How technology is changing the future of espionage. Available at: https://thenewsrep.com/40315/technology-changing-future-espionage/#ixzz3imhEq0HG [accessed 23 February 2018].

the target online: '[do they] repeatedly visit the same understated but elegant hotel on Amalfi Coast? What a coincidence! *That's my favorite hotel too. We have so much to talk about.*'[152]

Problems arise, however, if the target protects their social media accounts through privacy settings, limiting content to approved 'friends'. In theory, recruiters could circumvent this problem by joining a target's friends network, but that could advertise their relationship to counterintelligence, not to mention the fact that they would first need to gain their target's trust. MI5 sent guidance to the UK government after it found "a large number of HMG employees connected to known hostile foreign intelligence service cover profiles" on LinkedIn, showing that counterintelligence services do monitor these spaces for suspicious connections.[153] To circumvent this problem, Chinese intelligence created a fake social media account claiming to be the senior NATO commander at the time, US Admiral James Stavridis.[154] They then sent out 'friend' requests and personal messages to Stavridis' actual colleagues, granting Chinese operatives access to the personal profiles of a wide array of targets, including British military officers and Ministry of Defense officials.[155] This less than subtle tactic may have worked at the time, but it bears note that if discovered, such an act could easily alarm the target or attract counterintelligence.

A far more intrusive window into a target's private affairs may be gleaned through hacking.[156] This includes largescale data breaches, against organisations that

[152] Brenner, J. *America the vulnerable: inside the new threat matrix of digital espionage, crime, and warfare* (New York, The Penguin Press, 2011), p. 167.
[153] Drury, I. & Williams, D. (10 August 2015) Foreign spies on LinkedIn trying to recruit civil servants by 'befriending' them before stealing British secrets, *Daily Mail*. Available at: https://www.dailymail.co.uk/news/article-3191733/Foreign-spies-LinkedIn-trying-recruit-civil-servants-befriending-stealing-British-secrets.html [accessed 12 March 2018].
[154] Lewis, J. (10 March 2012) How spies used Facebook to steal NATO chiefs' details, *The Telegraph*. Available at: https://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefs-details.html [accessed 16 March 2019].
[155] Ibid.
[156] Gioe, D. V. 'The more things change', p. 218.

maintain vast databases of personal information. Incidents such as the 2014 Office of Personnel Management breach, for example, can reveal 'troves of personal information that would save any intelligence service untold amounts of time in seeking the right approach to recruit the right person, in the right agency, at the right time.'[157] For Chinese intelligence, the OPM breach was invaluable, as former US counterintelligence chief, Michelle Van Cleave, testified to Congress:

> The Chinese now have a detailed roster of most if not all American contractors and government employees who have access to classified information, plus a roster of their friends, colleagues or co-workers who may be useful conduits or potential assets in their own right … [they] also have a treasure trove of data that can be used to coerce, blackmail or recruit U.S. sources'.[158]

Despite some outrage in Washington, the incident was seen by intelligence pundits as an impressive achievement by Chinese hackers, including by Clapper: '[you] have to kind of salute the Chinese for what they did. If we had the opportunity to do that, I don't think we'd hesitate for a minute.'[159] However, in many respects, OPM was just another example of a rising trend, as enormous datasets of personal information are increasingly pursued by a wide range of malicious actors for criminal and intelligence purposes.[160] And the gains are not limited to the public sector - when the popular dating website tailored specifically for adulterers, known as Ashley Madison, was hacked in 2013, intelligence officers trawled the publicly released files to identify potential

[157] Ibid.
[158] Van Cleave, M. (9 June 2016) Chinese intelligence operations and implications for U.S. national security, *U.S. - China Economic and Security Review Commission.* Available at: http://www.uscc.gov/sites/default/files/Michelle%20Van%20Cleave_Written%20Testimony060916.pdf [accessed 31 November 2017], p. 4.
[159] NBC News (25 June 2015) China is 'leading suspect' in OPM hacks, says intelligence chief James Clapper. Available at: http://www.nbcnews.com/tech/security/clapper-china-leading-suspect-opm-hack-n381881 [accessed 1 March 2018].
[160] A fairly damming list of large-scale breaches is provided by CSO, with several of the incidents affecting over half a billion customers each. The biggest breach was that of *Yahoo*, between 2013-2014, a loss that impacted the personal data of *3 billion* accounts. For more details, see CSO from IDG (17 April 2018) The 18 biggest data breaches of the 21st century. Available at: https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html [accessed 23 December 2018].

sources, as well as to ensure that their own people had not been compromised.[161] Although the stolen data was largely used to uncover cheating spouses, such information could clearly have been used for recruitment purposes, as one practitioner affirmed: "knowing as much as possible about what's missing from their lives and what they are doing to fill it is of potential interest."[162]

But despite the media attention largescale breaches often generate, in reality these events are complex and far from guaranteed to succeed. Many occur due to negligence, a point underscored by the former presidential cyber security advisor, Richard Clarke, who quipped in 2002 that companies who spend more on coffee than security deserve to be hacked.[163] Companies such as Google spend millions of dollars on cyber security, but many corporations balk at such costs.[164] Even the OPM case reflects a federal failure to invest in the infrastructure, training, and resources needed for an effect defence, as Scot et al demonstrate:

> OPM failed because it lacked a fully implemented governance structure, it failed to properly assess system vulnerabilities, and it did not use robust authorization mechanisms. Many agencies still have inconsistent implementations of agreed upon governance frameworks for information security and ineffective system assessment and authorization mechanisms.
>
> OPM's lack of a cohesive vision and direction on how to best protect its systems/data, including the types of resources, skillsets, and tools needed, demonstrated that well-meaning personnel when tasked with IT tasks outside their regular professional core competencies are just as dangerous as malicious insider threats. Agencies need to employ trained IT staff to maintain systems and trained cybersecurity staff to work with IT and maintain information

[161] Farmer, B. (31 August 2015) British spies trawl Ashley Madison leak for intelligence, *The Telegraph.* Available at: http://www.telegraph.co.uk/news/uknews/defence/11830594/British-spies-trawl-Ashley-Madison-leak-for-intelligence.html [accessed 1 March 2018].
[162] Ibid.
[163] Clarke, R. A. & Knake, R. K. *Cyber war: the next threat to national security and what to do about it,* [Kindle version] (New York, HarperCollins, 2010). Accessed 20 June 2020, p. 130.
[164] Meyer, D. (29 January 2016) Here's how much Google paid out to security researchers last year, *Fortune.* Available at: https://fortune.com/2016/01/29/heres-how-much-google-paid-out-to-security-researchers-last-year/ [accessed 12 May 2020]; Brenner, J. *America the vulnerable,* p. 70; Gartzke, E. & Lindsay, J. R. 'Weaving tangled webs: offense, defense, and deception in cyberspace', *Security Studies,* 24:2, 2015, p. 323 – 326.

security protocols.[165]

Notwithstanding OPM's failings at the time, the incident was a harsh reminder for nations around the world that hacking could threaten all aspects of the state, thus necessitating a more robust approach to cybersecurity. Largescale breaches of government systems, particularly in the West, are often tied to outdated defences, as one NATO official complained, "[we've] layered on so many things [to legacy systems] that there are many attack levels across our networks."[166] And in the aftermath of OPM, the US government introduced sweeping reforms to 'improve the resilience' of its federal networks and update its antiquated defences.[167] Similarly, while British officials were assured that 'there was no single database in the UK with the same amount of detail', in 2018 the government announced its own 'cyber security standards', setting mandatory security standards for civil service organisations who protect sensitive information.[168] Western states are not the only actors attempting to modernise their cybersecurity programmes, as underscored in a 2018 speech by China's President Xi Jinping.[169] In his comments, that were not fully publicised, President Xi advocated an ambitious cybersecurity strategy:

> We must establish a correct cybersecurity view; strengthen cybersecurity protection of information infrastructure; strengthen the construction of comprehensive cybersecurity and information coordination mechanisms,

---

[165] Scott, J. et al. 'Preparing the battlefield: The coming espionage culture post OPM breach', *Institute for Critical Infrastructure,* 2015, p. 11.
[166] Brown, N. 'The path towards NEC: France, Germany and the United Kingdom', in *Technological Innovation and Defence: The Forza NEC Program in the Euro-Atlantic Framework*, edited by Alessandro Marrone, Michele Nones and Alessandro R. Ungaro (Roma, Edizioni Nuova Cultura, 2016), p. 75.
[167] OPM.gov (9 July 2015) OPM announces steps to protect federal workers and others from cyber threats. Available at: https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/ [accessed 1 March 2017]
[168] Cabinet Office (925 June 2018) Minimum cyber security standard. Available at: https://www.gov.uk/government/publications/the-minimum-cyber-security-standard [accessed 25 May 2020]; Corera, G. (7 April 2016) The spies of tomorrow will need to love data, *Wired*. Available at: http://www.wired.co.uk/article/spies-data-mi6-cia-gordon-corera [accessed 11 January 2018].
[169] New America (30 April 2018) Translation: Xi Jinping's April 20 speech at the National Cybersecuirty and Informatization work conference. Available at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/ [accessed 23 November 2018].

> methods, and platforms; strengthen the construction of cybersecurity incident response command capabilities; vigorously develop cybersecurity industries; move out in front; and prevent all possible trouble…
>
> …We must deeply launch cybersecurity and knowledge technology propaganda and dissemination, and raise the broad popular masses' cybersecurity consciousness and protection capabilities.[170]

As Greg Austin of the EastWest institute argues, these measures are intended to redress the fact that, regardless of its success as an offensive cyber actor, Chinese cybersecurity remains 'weak to very weak'.[171] It is indicative, that while the government relies on universities for its cybersecurity skills, none of its institutions offer 'world class' teaching in the subject area.[172] However, as an authoritarian regime, China may have more leverage to implement tougher security measures and enforce expensive modernisation programmes.[173] Indeed, China has tried to improve private sector defences by effectively reclassifying companies who store vast amounts of personal data as 'critical infrastructure', and those affected must implement robust defensive policies and be subjected to annual security reviews.[174]

Echoing China's concerns, Russia is pushing forward its own comprehensive strategy to modernise its archaic legacy systems.[175] Prior to 2017, Russia's cyber defences were notoriously weak, contrary to its otherwise impressive offensive capabilities.[176] As noted by senior FSB official, Dmitry Shalkov, Russian critical

---

[170] Ibid.
[171] Austin, G. (11 July 2018) How good are China's cyber defences? *The Diplomat.* Available at: https://thediplomat.com/2018/07/how-good-are-chinas-cyber-defenses/ [accessed 23 November 2018].
[172] Ibid.
[173] As Stoddart argues, with respect to cyber defences, 'authoritarian states might be better placed in combatting the threats now being faced because accountability and concerns of civil society in these states are subservient to perceived national interests'. For more details, see Stoddart, K. 'Live free or die hard: U.S.-UK cybersecurity policies.' *Political Science Quarterly*, 131:4, 2016, p. 804.
[174] Yang, Y. (30 May 2017) China's cybersecurity law rattles multinationals, *Financial Times.* Available at: https://www.ft.com/content/b302269c-44ff-11e7-8519-9f94ee97d996 [accessed 1 March 2018].
[175] Meduza (19 July 2017) Moscow's cyber-defense: how the Russian government plans to protect the country from the coming cyberwar. Available at: https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense [accessed 15 March 2017].
[176] Ibid.

infrastructure was attacked 70 million times in 2016 alone.[177] But since 2015, and driven by rising anticipation of a cyber conflict with NATO, the Kremlin has directed Moscow's scientific resources, and a small army of coerced hackers, to develop cutting edge defensive (and offensive) capabilities.[178] In further parallel to China, Russia has also forced the private sector to improve its own defences through strict legislation.[179] This includes changing the state's definition of critical infrastructure to include healthcare, communication, banking, energy, transport and other strategically valuable sectors.[180] This means, as Sergei Sukhankin of the Jamestown Foundation contends, that 'the Russian state will be able to exercise even greater control over public and private entities employing IT technologies and infrastructure.'[181] Every company on the list is obliged to bolster its cyber defences and report all detected intrusions to the government, as part of a national effort to counteract what the Kremlin views as increasing American efforts to collect Russian personal data. [182] And any company that uses insecure foreign software has now been warned, by Putin himself, that they will be banned from working with government agencies.[183]

Improved cyber defences can substantially increase the costs to hackers, or

[177] Sukhankin, S. 'Russia on the verge of a 'cyber purge?'', *The Jamestown Foundation*, 14:16, 2017. Available at: https://jamestown.org/program/russia-verge-cyber-purge/ [accessed 12 May 2020].
[178] Meduza (19 July 2017) Moscow's cyber-defense: how the Russian government plans to protect the country from the coming cyberwar. Available at: https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense [accessed 15 March 2017].
[179] Fripp, W. 'The hacked world order: how nations fight, trade, maneuver, and manipulate in the digital age', *Intelligence and National Security*, 33:4, 2018, p. 625.
[180] Russia Today (12 July 2017) Duma passes bill on protection of Russian state data networks. Available at: https://www.rt.com/politics/396096-duma-passes-bill-on-protection/ [accessed 1 March 2018].
[181] The Jamestown Foundation (February 9 2017) Russia on the verge of a 'cyber purge?' Available at: https://jamestown.org/program/russia-verge-cyber-purge/ [accessed 4 January 2020].
[182] Russia Today (25 January 2017) 70m cyberattacks, mostly foreign, targeted Russia's critical infrastructure in 2016 – FSB. Available at: https://www.rt.com/news/374973-cyber-attacks-russian-infrastracture/ [accessed 1 March 2018].
[183] Reuters (8 September 2017) Putin tells Russia's tech sector: ditch foreign software or lose out. Available at: https://uk.reuters.com/article/russia-it-software/putin-tells-russias-tech-sector-ditch-foreign-software-or-lose-out-idUKL8N1LP4IC [accessed 23 June 2020]; Mondaq (31 October 2018) Russian Federation: privacy and security in Russia. Available at: http://www.mondaq.com/russianfederation/x/750216/Data+Protection+Privacy/Privacy+And+Cybersecurity+In+Russia [accessed 16 March 2019].

simply render certain breaches unfeasible. Even against OPM's deficient defences, Chinese hackers took over a year to carefully remove their data, and, as experts noted, if best-practice security measures were in place beforehand, the breach might have been stopped in its tracks.[184] For example, the application of strong encryption could have at least mitigated its impact, since without the corresponding keys stolen information would have been unreadable.[185] Similarly, when the medical insurance firm *Anthem* was hacked in 2015, it too was criticised for the fact that such highly sensitive information had not been encrypted.[186] It is possible for hackers to acquire encryption keys, but systems such as multifactor authentication (requiring more than one key) or biometric locks, add extra layers of frustration and complication for intruders (these measures were introduced by OPM in 2015, at the point when their data was already exposed).[187] Intelligence officers could recruit insider sources to provide the required encryption keys or biometric prints, a point underscored by former CIA officer Henry Crumpton, who notes that 'people', including those who knew the passwords, encryption keys, or firewall software, were all important targets when pursuing systems.[188] However, one common security practice is known as the 'two person rule',

[184] Scott, J. et al. 'Preparing the battlefield', p. 11.
[185] Perera, D. (4 June 2015) Agency didn't encrypt feds' data hacked by Chinese, *Politico*. Available at: https://www.politico.com/story/2015/06/personal-data-of-4-million-federal-employees-hacked-118655 [accessed 23 January 2020].
[186] Zetter, K. (2 May 2015) Health insurer anthem is hacked, exposing millions of patients' data, *Wired*. Available at: https://www.wired.com/2015/02/breach-health-insurer-exposes-sensitive-data-millions-patients/ [accessed 19 March 2019].
[187] Scott, J. et al. 'Preparing the battlefield', p. 14-16; GAO, 'Information security: OPM has improved controls, but further efforts are needed', *U.S. Government Accountability Office*, 2017, p. 16.
[188] One glaring question here is why bother recruiting a source to provide encryption keys, when you could simply recruit a source to provide personal data? Due to internal security practices that are discussed in more detail in chapter 6, it is surprisingly difficult for employees to actually view or download personal data without being noticed. For example, only a handful of Facebook employees can access its customers' private data, and those who do are tightly monitored. Similar if not more stringent practices can be seen in the public sector. The UK government requires intelligence agencies to protect personal information through 'physical security', 'IT security', and a 'security clearance regime which is designed to provide assurance that those who have access to this material are reliable and trustworthy'. From 2014 to 2016, two employees from MI5 and three from MI6 were disciplined for mishandling data, while one GCHQ employee was fired for a similar offense. For more details, see Crumpton, H. A. *The art of intelligence: lessons from a life in the CIA's clandestine service*, (Penguin Books 2012), p. 79; Seetharaman, D. (3 May 2018) Facebook's double standard on privacy: employees vs. Everyone else,

which requires the keys of multiple persons to access certain data, a practice that would render a single insider source redundant.[189] It is thus unsurprising that China's new security rules require any companies who collect, store, or share personal data, to protect that information through robust encryption.[190]

However, no amount of legislation can ensure infallible defences, allowing cracks for Western intelligence agencies to exploit. Two years after President Xi's cybersecurity speech, China continues to be wracked by personal data breaches.[191] Most have occurred in the private sector, where enforcement of its new legal measures has been weak and an illicit market for personal information has thrived. The authorities suspect that about 1.5 million people are domestically and illegally trading personal information, much of which is pilfered from mobile phone applications.[192] Likewise, in 2019, a BBC investigation into Russia's prolific and growing personal data 'black market' found that for 'a modest fee, you can gain access to mobile phone records, addresses, passport details, and even bank security codes.'[193] Many of these leaks originate from corrupt government officials trying to 'supplement their often

The Wall Street Journal. Available at: https://www.wsj.com/articles/facebooks-double-standard-on-privacy-employees-vs-the-rest-of-us-1525383859 [accessed 4 May 2018]; Home Office (December 2017) Intelligence services' retention and use of bulk personal datasets. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668933/Draft_BPD-_Intelligence_Services__Retention_and_Use_of_Bulk_Personal_Datasets.pdf [accessed 1 March 2018]. p. 38; Bowcott, O & Norton-Taylor, R. (21 April 2016) UK spy agencies have collected bulk personal data since 1990s, files show, *The Guardian.* Available at: https://www.theguardian.com/world/2016/apr/21/uk-spy-agencies-collected-bulk-personal-data-since-1990s [accessed 1 March 2018].

[189] Cappelli, D. Moore, A. Trzeciak, R. *The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud),* (Boston, Addison-Wesley, 2012), p. 58

[190] Carnegie (30 May 2019) The encryption debate in China. Available at: https://carnegieendowment.org/2019/05/30/encryption-debate-in-china-pub-79216 [accessed 12 July 2020].

[191] NPR (5 January 2020) In China, a new call to protect data privacy. Available at: https://www.npr.org/2020/01/05/793014617/in-china-a-new-call-to-protect-data-privacy?t=1600710014451 [accessed 12 May 2020].

[192] Ibid.

[193] BBC News (27 May 2019) Russian data theft: shady world where all is for sale. Available at: https://www.bbc.co.uk/news/world-europe-48348307 [accessed 12 May 2020].

meagre wages'.[194] But according to Meduza, negligence also plays an important role, with some of Russia's most important strategic agencies beleaguered by a trend of cybersecurity incompetence.[195] However, as the protection of personal information rises up the agenda, both regimes have greater incentive to clamp down on negligence, corruption, and incompetence, as illustrated by crackdowns down in China on data leakers.[196] Therefore, while breaches akin to the OPM hack may be just as appealing to SIS or the CIA as they are to their opponents (as Clapper conceded), those same agencies are more likely to be obstructed by increasing cyber defences. Cracks may occur, but it is clear that Russia and China are determined to protect the most appealing targets, especially from the hands of foreign intelligence.

If largescale breaches are to occur, they are more likely to succeed against the private sector, where negligence is more commonplace. But this raises serious political implications, particularly at a time when the West is keen to dissuade its competitors from rampant economic hacking.[197] In 2020, Chinese security firm Qihoo released evidence tying Langley to a series of breaches against airlines and industries throughout China, only a month after the US indicted four of Beijing's military hackers.[198] Moreover, considering the difficulties in determining the motive behind a hack - to repeat a point made in chapter two, OPM offered both offensive and defensive

[194] Ibid.
[195] Meduza (19 July 2017) Moscow's cyber-defense: how the Russian government plans to protect the country from the coming cyberwar. Available at: https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense [accessed 15 March 2020].
[196] Security Magazine (16 August 2019) China cracking down on data theft caused by mobile apps. Available at: https://www.securitymagazine.com/articles/90732-china-cracking-down-on-data-theft-caused-by-mobile-apps [accessed 12 May 2020].
[197] In 2020, the EU introduced sanctions against Russia, China, and North Korea for a series of past hacking attacks, including WannaCry and Operation Cloud Hopper. For more details, see ZDNet (30 July 2020) EU sanctions China, Russia, and North Korea for past hacks. Available at: https://www.zdnet.com/article/eu-sanctions-china-russia-and-north-korea-for-past-hacks/ [accessed 24 August 2020].
[198] Reuters (3 March 2020) Chinese cybersecurity company accuses CIA of 11-year-long hacking campaign. Available at: https://www.reuters.com/article/us-china-usa-cia-idUSKBN20Q2SI [accessed 12 May 2020].

advantages to Chinese intelligence - there is always a risk that a breach may be misconstrued or incur some form of retaliation.[199] Given that Obama's administration instructed the NSA to hack Russian networks in response to its 2016 DNC breach, and that some US politicians called for a similar response to China over OPM, it can be assumed that foreign opponents might respond in kind.[200] As security specialist Emilio Lasiello adds, nations now assume that 'being able to "out hit" an aggressor in cyberspace will invariable cause the offending activity to stop and for the aggressor to look elsewhere for a victim.'[201] Those risks are unlikely to deter largescale breaches altogether, but they are also unlikely to be discounted.

However, in 2017 a batch of documents released by Wikileaks, dubbed Vault 7, showed that Langley had developed a sophisticated catalogue of tools for hacking popular smartphones and other personal devices.[202] By hacking an individual's personal device, reams of personal information can be surreptitiously pilfered, including financial details, photographs, contacts, usernames and passwords, social media accounts, private documents, and communication logs.[203] Some of the CIA's tools could even bypass the encryption of popular instant messengers, including WhatsApp, Telegram, and Signal, lifting the cleartext logs from a target's phone.[204] The files also exposed the CIA's ability to siphon a smartphone's audio, video, and geo-locational

[199] Sebenius, A. (28 June 2017) Writing the rules of cyberwar, *The Atlantic.* Available at: https://www.theatlantic.com/international/archive/2017/06/cyberattack-russia-ukraine-hack/531957/ [accessed 10 January 2018].
[200] Sanger, D. E. (31 July 2015) U.S. decides to retaliate against China's hacking, *The New York Times.* Available at: https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html [accessed 10 January 2018].
[201] Tech Native (10 July 2018) Retaliatory hacking has returned – will states ever learn? Available at: https://www.technative.io/retaliatory-hacking-has-returned-will-states-ever-learn/ [accessed 12 May 2020].
[202] Wikileaks (7 March 2017) Press release. Available at: https://wikileaks.org/ciav7p1/index.html [accessed 1 March 2018].
[203] Schneier, B. *Carry on sound advice from Schneier on Security,* (Indianapolis, John Wiley & Sons, Incorporated, 2013), p. 119.
[204] For more details, see Barrett, B. (7 March 2017) Don't let WikiLeaks scare you off of Signal and other encrypted chat apps, *Wired*. Available at: https://www.wired.com/2017/03/WikiLeaks-cia-hack-signal-encrypted-chat-apps/ [accessed 10 January 2018].

data without alerting the device's operator.[205] In one sense this is comparable to planting a listening device, but unlike a traditional bug, an infected smartphone is likely to travel with its owner.[206] The prospect of turning a target's personal device into a mobile surveillance platform is undoubtedly a tempting one, as one former US diplomat affirmed, "[everything] with bugs has been tried, phones are better".[207] Theoretically, intelligence officers could listen in on the target's conversations in work, at home, or while engaging in some private indiscretion, and even watch these events play out with the aid of the smartphone's camera.

However, while Langley's hacking tools have inevitably evolved since the leak, Vault 7 revealed a heavy dependence on 'zero day' exploits.[208] Zero day exploits are considered one of the most powerful tools in a hacker's arsenal, because they use flaws in code that are unknown to 'software makers and to the antivirus vendors'.[209] As one former NSA hacker explains, "since no one knows except the attacker about the [exploits]" there are no means to detect or block them.[210] The downside for hackers, is that because they can offer unimpeded access to systems, they are just as highly sought

[205] Similar capabilities appear to be available to British intelligence. Snowden claimed that GCHQ used a series of capabilities dubbed the "Smurf Suite" These, as Snowden described in a BBC interview, could access "who you call, what you've texted, the things you've browsed, the list of your contacts, the places you've been, the wireless networks that your phone is associated with … And they can do much more, they can photograph you." If such capabilities were available to GCHQ, it could be suggested that the same capabilities may be shared with SIS. For more details, see BBC News (5 October 2015) Edward Snowden interview: 'smartphones can be taken over'. Available at: http://www.bbc.co.uk/news/uk-34444233 [accessed 1 January 2018]; Wikileaks (7 March 2017) Press release. Available at: https://wikileaks.org/ciav7p1/index.html [accessed 1 March 2018].
[206] As Michalevsky et al contend, '[in] effect, tracking the location of a phone is practically the same as tracking the location of its owner.' For more details, see Michalevsky, Y. et al. 'PowerSpy: Location tracking using mobile device power analysis', *24th Usenix Security Symposium*, 2015, p. 1.
[207] Kupfer, M. & Bodner, M. (19 January 2017) Spy games: how the spectre of surveillance impacts Moscow's foreigners, *The Moscow Times*. Available at: https://themoscowtimes.com/articles/spy-games-how-the-spectre-of-surveillance-impacts-the-lives-of-moscows-foreigners-56865 [accessed 13 February 2018].
[208] Greenberg, A. (7 March 2017) How the CIA can hack your phone, PC, and TV (says Wikileaks), *Wired*. Available at: https://www.wired.com/2017/03/cia-can-hack-phone-pc-tv-says-wikileaks/ [accessed 1 December 2017].
[209] Zetter, K. *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon,* [Kindle version] (New York, Crown Publishers, 2014). Accessed 23 May 2020, p. 8.
[210] O'Harrow Jr. R. *Zero day: the threat in cyberspace*, [Kindle version] (New York, Division Books, 2013). Accessed 23 May 2020, p. see Introduction.

after by the defending side.[211] This is especially true for popular consumer brands, with companies such as Apple, Facebook, and Google willing to pay enormous fees for any uncovered flaws in their code.[212] For example, the zero day research company *Zerodium* offers up to $2.5 million for flaws in Android, up to $1.5 million for flaws in iPhones and WhatsApp, and a modest $500,000 for Telegram, Signal, and WeChat.[213] Hence, in a lucrative market, zero days are likely to be more difficult to discover while yielding shorter lifespans, turning even smartphones into hacking hard targets. Indeed, both Apple and Google were quick to reassure their customers that the zero days found in Vault 7 had been patched years beforehand.[214]

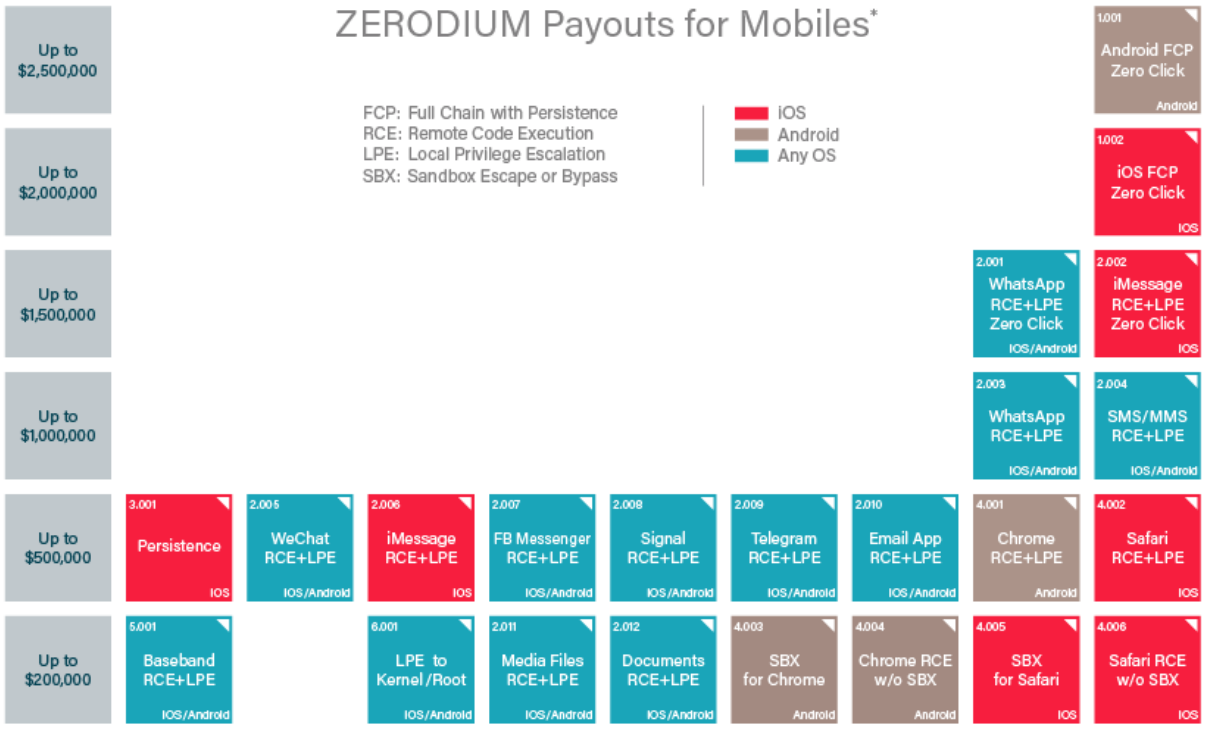

Figure 1: Sample of Zerodium malware pay-outs.[215]

[211] Greenberg, A. (18 November 2015) Here's a spy firm's price list for secret hacker techniques, *Wired*. Available at: https://www.wired.com/2015/11/heres-a-spy-firms-price-list-for-secret-hacker-techniques/ [accessed 1 January 2018].
[212] Ibid.
[213] Zerodium - Our exploitation acquisition program. Available at: https://zerodium.com/program.html [accessed 23 May 2020].
[214] Burgess, M. (7 May 2017) Wikileaks drops 'Grasshopper' documents, part four of its CIA Vault 7 files, *Wired*. Available at: https://www.wired.co.uk/article/cia-files-wikileaks-vault-7 [accessed 1 March 2018].
[215] Zerodium - Our exploitation acquisition program. Available at: https://zerodium.com/program.html [accessed 23 May 2020].

Moreover, to ensure a high standard of security for their employees, governments may invest in secure work phones. In 2017, Russia supplied 50,000 employees of companies co-owned by the state with so-called 'Taiga phones', that are purpose built to protect operators from sophisticated hacking threats.[216] It is telling that *RT News* describes the Russian smartphones as 'totally surveillance-proof', offering 'unparalleled, corporate-level' security.[217] Such claims may be overblown by the state-sponsored news service, but on paper the device offers an abundance of advantages, including multiple levels of cyber defences that allegedly block data from being siphoned by rogue software.[218] In addition, the device supposedly alerts the user and disables key systems, including its camera, GPS, and microphone, when an intrusion is detected.[219] And in addition to allegedly banning government officials from using phones built by foreign companies such as Apple and Samsung (for security reasons), China is developing a secure smartphone of its own.[220] Built by domestic firms to evade malicious tampering in manufacturing, the phone is intended for its federal workers, maximising security by purportedly lacking cameras, Wi-Fi, GPS, and Bluetooth.[221] Thus, the most valuable targets, namely the phones of government and defence

[216] Bloomberg (25 September 2017) Natalya Kaspersky's snoop-proof phone helps Putin thwart spies. Available at: https://www.bloomberg.com/news/articles/2017-09-25/natalya-kaspersky-s-snoop-proof-phone-helps-putin-thwart-spies [accessed 1 March 2018].
[217] RT News (19 February 2015) 'Unhackable': Russian firm develops totally surveillance-proof smartphone. Available at: https://www.rt.com/news/233723-russian-phone-security-encryption/ [accessed 1 December 2018].
[218] Bloomberg (25 September 2017) Natalya Kaspersky's snoop=proof phone helps Putin thwart spies. Available at: https://www.bloomberg.com/news/articles/2017-09-25/natalya-kaspersky-s-snoop-proof-phone-helps-putin-thwart-spies [accessed 1 March 2018].
[219] RT News (19 February 2015) 'Unhackable': Russian firm develops totally surveillance-proof smartphone. Available at: https://www.rt.com/news/233723-russian-phone-security-encryption/ [accessed 1 December 2018].
[220] Quartz (24 September 2014) If China really is banning official use of Apple and Samsung phones, here's who benefits. Available at: https://qz.com/270351/if-china-really-is-banning-official-use-of-apple-and-samsung-phones-heres-who-benefits/ [accessed 1 January 2018]; Dou, E. & Osawa, J. (20 November 2015) China to build its own secure smartphones, *The Australian.* Available at: https://www.theaustralian.com.au/business/business-spectator/china-to-build-its-own-secure-smartphones/news-story/2ca15fd9c3683ae36fc8a1bb5da7c7c8 [accessed 1 March 2018].
[221] Ibid.

officials, are also likely to be the most well defended.

However hacking is not constrained to smartphones and personal computers, with increasingly interconnected home environments opening more pathways into a target's private space.[222] This is personified by the so-called 'Internet of Things', whereby multiple hackable devices ranging from thermostats, to fridges, televisions, and even cars, all interact within a home network.[223] For instance, hackers might first gain access to thermostat, as an entry point to 'security cameras or computers connected to the same network.'[224] Furthermore, home entertainment smart hub systems like Siri or Alexa can offer reams of personal data.[225] According to Schnader, Alex offers a 'veritable treasure trove for a foreign government seeking information on a specific person. Foreign agents could extract user data, including voice recordings, and bank account information; manipulate the environment of a target's home; or even surreptitiously record audio or video.'[226] Similarly, the hacking of Fitbits and similar fitness devices have been used to track movements and physical fitness, data that could yield dividends about a person's suitability for high-stress espionage, or even reveal their whereabouts.[227] Given these opportunities, it is perhaps unsurprising that the Vault 7 disclosures revealed a range of CIA hacking toolkits aimed at wider devices,

[222] Fischer, E. A. 'The Internet of Things: Frequently Asked Questions', *Congressional Research Service*, 2015. Available at: http://www.fas.org/sgp/crs/misc/R44227.pdf [accessed 23 May 2020], p. iii.
[223] Ibid, p. 14.
[224] Ibid.
[225] Schnader, J. 'Alexa, are you a foreign agent? Confronting the risk of foreign intelligence exploitation of private home networks, home assistants, and connectivity in the security clearance process', *Richmond Journal of Law & Technology*, 25:4, 2019, p. 7.
[226] Ibid.
[227] Cyr, B, Horn, W., Miao, D., Specter, M. 'Security analysis of wearable fitness devices (Fitbit)' *Massachusetts Institute of Technology* (MIT), 2014, pp. 1-14; Wikileaks (March 2017) Weeping angel (extending) engineering notes. Available at: https://wikileaks.org/ciav7p1/cms/page_12353643.html [accessed 1 March 2018]; CNBC (8 January 2016) There's a hack for that: Fitbit user accounts attacked. Available at: https://www.cnbc.com/2016/01/08/theres-a-hack-for-that-fitbit-user-accounts-attacked.html [accessed 12 May 2020].

including smart televisions, and, in some cases, smart cars.[228] One of these toolkits, named 'Weeping Angel' targeted Samsung televisions, accessing their embedded microphones while harvesting Wi-Fi details and passwords to facilitate further penetration of home networks.[229] However, while many household devices remain vulnerable, manufacturers are slowly adapting to security threats, meaning some of the more popular brands may prove harder to breach.[230]

Since security measures are likely to raise the costs of brute force hacking, substantial effort can be saved by circumventing a device's defences. One way to do so is social engineering, a repurposed term that often refers to the duping of targets for hacking purposes.[231] 'Phishing' is a common example of social engineering, whereby hackers use fake emails designed to imitate legitimate sources, to exploit the target's trust and solicit certain actions, such as downloading infected files.[232] The former Director of the CIA's National Clandestine Service, Michael Sulick, demonstrates how social engineering can be applied by intelligence officers:

> In the cyber realm, once a Russian intelligence officer identifies a target, he then fabricates a profile that will appeal based on common interest, usually not related to the target's work and access to secrets so that the contact appears non-threatening. He may establish a connection with the target directly or, to enhance his credibility, he may instead develop a relationship with a friend or follower of the target who shares the same interest and, later, he uses this unwitting intermediary to establish his bona fides. Once the relationship with the target matures, the Russian intelligence officer sends him a "phishing" message with a link or attachment. With one simple click by the credulous target, Russian intelligence gains access to his computer holdings. The tactic works. Russian intelligence reportedly used social media accounts in its phishing email attacks that penetrated the Pentagon in 2015.[233]

[228] Greenberg, A. (7 March 2017) How the CIA can hack your phone, PC, and TV (says Wikileaks), *Wired*. Available at: https://www.wired.com/2017/03/cia-can-hack-phone-pc-tv-says-wikileaks/ [accessed 1 December 2017].
[229] Wikileaks (March 2017) Weeping angel (extending) engineering notes. Available at: https://wikileaks.org/ciav7p1/cms/page_12353643.html [accessed 1 March 2018].
[230] Consumer Reports (7 February 2018) Samsung and Roku smart TVs vulnerable to hacking, consumer reports finds. Available at: https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/ [accessed 23 March 2020].
[231] Lucas, E. *Cyberphobia*, p. 113.
[232] Ibid.
[233] The Cipher Brief (30 January 2016) Espionage and social media. Available at:

However, while some experts have touted social engineering as the 'art of human hacking', its leverage should not be overvalued. In the 2015 Pentagon case cited by Sulick, the Russian hackers only succeeded in socially engineering defence personnel by trawling social media for information about those employees.[234] In other words, they depended on information gathered from open sources to enhance the con, making their approaches appear more realistic and trustworthy.[235] That, therefore, assumes that the hacker can find enough personal information to make social engineering possible. In another illustrative case, Iranian hackers relied on personal information provided by the US defector, Monica Witt, in order to socially engineer US Airforce personnel.[236] Using "target packages" supplied by Witt (a former US Airforce intelligence specialist), the Iranians created fake Facebook profiles carefully constructed to lure her colleagues into downloading malicious file attachments.[237] But without Witt's input, the Iranian operation may never have succeeded.

It is also likely that Russia and China will train key employees against the risks of social engineering, similar to the way the US government informs its personnel through programmes such as "Know the Risk Raise your Shield".[238] However, while trained targets will prove harder to dupe, family members may offer opportunities. As cyber security specialist Jayson Street argues, "[why] not compromise the wife's

https://www.thecipherbrief.com/column_article/espionage-and-social-media [accessed 1 January 2018].
[234] CRN (7 August 2015) Pentagon data breach shows growing sophistication of phishing attacks. Available at: https://www.crn.com/news/security/300077701/pentagon-data-breach-shows-growing-sophistication-of-phishing-attacks.htm [accessed 23 May 2020].
[235] Ibid.
[236] 'United States of America v. Monica Elfriede Witt, Mojtaba Masoumpour, Behzad Mesri, Hossein Parvar, and Mohamad Paryar', *Department of Justice*, 2018, p. pp. 1-27.
[237] Shubber, K. (13 February 2019) Former US Air Force agent charged with spying for Iran, *Financial Times*. Available at: https://www.ft.com/content/54aa515e-2faa-11e9-8744-e7016697f225 [accessed 24 May 2020].
[238] Office of the Director of National Intelligence – Know the risk raise your shield: NSCS awareness materials. Available at: https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-awareness-materials [accessed 15 March 2017].

computer system and then, when [the target of interest] brings his laptop home, he is now on the internal network", adding "[the] home network is more of a private network, which is more trusted. And that means the firewall lets more stuff in. It makes more sense to compromise the [target] that way."[239] According to a 2016 Kaspersky Labs report, Russian citizens were often being webcam hacked due to poor cyber security practices, including an apparently common tendency to turn off antivirus software.[240] The naivety of a partner or child, therefore, might offer an ideal entry point, providing a window into the target's home.

Alternatively, many of the toolkits revealed by Vault 7, pertaining to smartphones and televisions alike, were described as 'close access'.[241] This means that physical access to the device was needed to circumvent security measures, implying the operative would need to somehow privately tamper with the device unnoticed.[242] Although it is unlikely that the CIA would be able to infect devices at the manufacturing level, especially in hard targets, the Vault 7 files revealed that operatives had been able to physically infect certain "factory fresh" devices, potentially by "interdicting mail orders and other shipments … leaving the United States or otherwise".[243] In fact, one report even suggests gifting a 'MacBook Air' to a target that has been ready 'implanted' with specific malware.[244] But the success of tampering with

[239] CSO Online (14 July 2014) 4 reasons why executives are the easiest social engineering targets. Available at: https://www.csoonline.com/article/2125311/social-engineering/4-reasons-why-executives-are-the-easiest-social-engineering-targets.html [accessed 1 March 2018].
[240] Kaspersky Daily (3 May 2016) Hackers broadcast live footage from hacked webcams on YouTube and trolls are loving it. Available at: https://www.kaspersky.co.uk/blog/2ch-webcam-hack/7120/ [accessed 25 May 2020].
[241] KrebsonSecurity (8 March 2017) Wikileaks dumps docs on CIA's hacking tools, Krebs on Security, 2017. Available at: https://krebsonsecurity.com/tag/vault-7/ [accessed 25 June 2020].
[242] Ibid.
[243] Reisinger, D. (23 March 2017) WikiLeaks says CIA targeted iPhone supply chain since 2008, *Fortune.* Available at: http://fortune.com/2017/03/23/apple-wikileaks-iphone/ [accessed 1 March 2018].
[244] CIA 'Engineering Development Group: DarkSeaSkies 1.0 User Requirements Documents, *Wikileaks*, 2009. Available at: https://wikileaks.org/vault7/darkmatter/document/DarkSeaSkies_1_0_URD/DarkSeaSkies_1_0_URD.pdf [accessed 24 May 2020], p, 1.

devices before security updates have been installed is questionable, with another report stating that some methods lack "stealth and persistence capabilities" – meaning that, once the phone is updated, the hack ceases to work.[245] Gaining access to an updated device is considerably more difficult, since operatives may need to surreptitiously enter the target's premises, a factor that is all the more problematic considering that many people keep their phones in close proximity. A safer solution, however, is targeting the personal devices of travelling officials, as security specialist Sean Sullivan notes, "[if] someone's going through airport security … a CIA agent would have the ability to put this on, track him around the world, hack a back door and the computer calls home to us."[246] This appears to be an established tactic, with Chinese border guards accused of bugging tourists phones with surveillance apps and downloading their personal information as they pass through Xinjiang's airports. It is a tactic CIA officers could mimic with the help of cooperative airport personnel.[247]

A more elaborate method, one performed by British intelligence, is to hack upmarket hotels used by foreign officials. As revealed in the Snowden files, a GCHQ programmed called *Royal Concierge* targeted over 350 international upscale hotels in support of HUMINT operations.[248] The programme, which ran for at least three years, provided automated alerts when foreign diplomats booked hotel reservations, by monitoring hotel networks for emails sent via "gov.xx" or specified addresses.[249] These

[245] Greenberg, A. (23 March 2017) Wikileaks reveals how the CIA can hack a mac's hidden code, *Wired*. Available at: https://www.wired.com/2017/03/wikileaks-shows-cia-can-hack-macs-hidden-code/ [accessed 1 March 2018].
[246] The Telegraph (20 May 2017) British and US spies at risk after WikiLeaks publishes top-secret CIA spyware document. Available at: https://www.telegraph.co.uk/news/2017/05/20/british-us-spies-risk-wikileaks-publishes-top-secret-cia-spyware/ [accessed 1 March 2018].
[247] Osborne, H. (2 July 2019) Chinese border guards put secret surveillance app on tourists' phones, *The Guardian.* Available at: https://www.theguardian.com/world/2019/jul/02/chinese-border-guards-surveillance-app-tourists-phones [accessed 14 January 2021].
[248] Poitras, V. L. et al. (17 November 2013) GCHQ monitors diplomats' hotel bookings, *Der Spiegel.* Available at: http://www.spiegel.de/international/europe/gchq-monitors-hotel-reservations-to-track-diplomats-a-933914.html [accessed 1 March 2018].
[249] Snowden Archive - Contact mapping – tip-off to Diplomatic travel plans. Available at:

alerts then become an ‘enabler for HUMINT’, allowing operatives to influence the target’s travel, or place someone on the ground ready to meet them.[250] And by knowing which hotels to target, intelligence officers could pre-emptively bug the traveller’s suite with listening devices, as Der Spiegel reports:

> A further document states that this advance knowledge of which foreign diplomats will be staying in what hotels provides GCHQ with a whole palette of intelligence capabilities and options. The documents reveal an impressive listing of capabilities for monitoring a hotel room and its temporary resident that seem to exhaust the creative potential of modern spying. Among the possibilities, of course, are wiretapping the room telephone and fax machine as well as the monitoring of computers hooked up to the hotel network ("computer network exploitation").
>
> It also states that a "Technical Attack" is deployed by the British "TECA" team for guests of high interest. The documents state that these elite units develop a range of "specialist technologies" that are "designed to bridge the gaps to communications that our conventional accesses cannot reach." These "Active Approach Teams" are small, but possess advanced technical skill that allow them to work within "often unique requirements."[251]

While it is not explicitly stated that GCHQ hacked hotel networks to identify “gov.xx” addresses (it may have also used passive surveillance), the option cannot be ruled out. This was precisely how another advanced group of hackers penetrated hotel networks in Russia, China, and several other countries, with a malware dubbed ‘DarkHotel’.[252] Once on the hotel’s network, guests would receive a seemingly legitimate software update message, which would then download malware, steal their data, and delete any trace of the initial infection.[253] But even if the guest didn’t download malware themselves, knowing the target’s hotel through programmes such as Royal Concierge would at least provide an opportunity to infect certain items safely. If the target leaves

https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH6d2f.dir/doc.pdf [accessed 1 March 2018].

[250] Poitras, V. L. et al. (17 November 2013) GCHQ monitors diplomats’ hotel bookings, *Der Spiegel*. Available at: http://www.spiegel.de/international/europe/gchq-monitors-hotel-reservations-to-track-diplomats-a-933914.html [accessed 1 March 2018].

[251] Ibid.

[252] BBC News (11 November 2014) DarkHotel hackers targets company bosses in hotel rooms. Available at: http://www.bbc.co.uk/news/technology-30001424 [accessed 1 March 2018].

[253] Ibid.

their laptop behind while setting out for lunch, operatives could enter the premises and infect the device in a matter of minutes. The downside, however, is that this only applies to those cases where hotels can be accessed safely, and would raise considerable complication in hard target conditions.

Accounting for all of the issues raised above, it is clear that cyber-enabled surveillance is hardly risk-free, which in turn pushes up the need for trust. Mainly, intelligence officers will need assurances that a person of interest would say or do something to merit surveillance's risks. With regards to open or semi-open sources, it did not take long before governments sought to protect sensitive personnel through rules and guidelines for social media.[254] These are common in the West - the US Department of Defense 'has five such programs', while the UK runs the "Think before you share' campaign for service members and MoD civilians.'[255] Aside from encouraging personnel to apply privacy settings to their social media accounts, these programmes instruct employees to be mindful of what they say and post within their public networks. [256] Similar, if not harsher, rules must be expected in authoritarian regimes - as previously noted, China monitors its soldiers through surveillance software, but Russia has adopted far more draconian measures in response to routine military leaking through social media.[257] In 2019, the Kremlin banned all servicemen from using smartphones (or other Internet-enabled personal devices), posting photos, or

[254] Gioe, D. V. 'The more things change', p. 219.
[255] Ibid; Ministry of Defence (22 October 2012) Using social media – a guide for military personnel. Available at: https://www.gov.uk/government/publications/using-social-media-a-guide-for-military-personnel [accessed 1 January 2018].
[256] As the UK's Think Before you Share programme advises '[whenever] you join a social network, you should always look at the privacy and security settings. Do this frequently as settings are subject to change. Each social network deals with privacy and security in different ways, and you shouldn't share information on their service until you know where that could end up.' For more details, see Gov.UK (21 October 2013) Think before you share online. Available at: https://www.gov.uk/guidance/think-before-you-share [accessed 12 May 2020].
[257] RT News (13 February 2018) Defense Ministry recommends Russian military quits using social networks – report. Available at: https://www.rt.com/politics/418629-defense-ministry-recommends-russian-military/ [accessed 1 March 2018].

writing about the military while on duty, at the risk of a two week jail sentence.[258] In that sense, Russia put its soldiers on the same footing as its security services, who were already banned from posting about themselves or their work online.[259] Consequently, although many Russian and Chinese officials are likely to have at least some openly visible online presence, intelligence officers are unlikely to learn a great deal from these spaces, at least beyond more mundane insights into a person-of-interest's life.

As for hacking, largescale database breaches are likely to produce an enormous amount of information, purely because citizens have essentially lost control over their data. That said, while personal information such as medical bills may be acquirable, there's no guarantee that a golden nugget – such as evidence that a Russian intelligence officer might be gay, which is still taboo inside conservative societies – is going to be found in some gigantic database. Targeted hacking is more likely to provide a hidden window into someone's personal affairs, but this too is also highly vulnerable to self-censorship. At minimum, it seems likely that those who work in intelligence and security circles will consider themselves targets of foreign eavesdropping and adjust their behaviours accordingly. FBI employees, as a case in point, place caps over their office webcams to block the view of anyone who might have hacked their systems.[260] The CIA, alternatively, simply bars its people from taking smartphones into the workplace, thus ensuring that compromised personal devices are kept safely distanced from sensitive conversations.[261] While Russian and Chinese intelligence officers are

[258] Meduza (6 August 2019) How and why the Russian military puts soldiers in jail for using smartphones and social media. Available at: https://meduza.io/en/feature/2019/08/06/how-and-why-the-russian-military-puts-soldiers-in-jail-for-using-smartphones-and-social-media [accessed 21 March 2020].
[259] This rule applies to at least the FSB and the FSO (Federal Protective Service). For more details, see BBC News (5 October 2017) Russian soldiers face ban on selfies and blog posts. Available at: http://www.bbc.co.uk/news/world-europe-41510592?ocid=socialflow_twitter [accessed 1 January 2018].
[260] CSIS - Transcripts – The national security division at 10. Available at: https://www.csis.org/transcripts-national-security-division-10 [accessed 1 March 2018].
[261] CIA (18 September 2015) Deputy Director Cohen delivers remarks on CIA of the future at Cornell University. Available at: https://www.cia.gov/news-information/speeches-testimony/2015-speeches-

likely to adopt similar precautions, it should also be considered that heavily surveilled regimes only encourage a culture of self-censorship amongst their citizenry.[262] According to *Surveillance Self Defense,* a project by the *Electronic Frontier Foundation*, persistent criminal and government smartphone hacking is already impacting cultural self-censorship, with some responding to concerns by 'moving mobile phones into another room when having a sensitive conversation, or by powering them off.'[263] And as noted earlier, an increasing number of Russian officials, who are paranoid about hacking from their own security services, have taken to removing the batteries from their phones whenever they discuss anything remotely sensitive. [264] Furthermore, according to current and former US intelligence officials, senior ranking members of the Kremlin are 'guarded in their use of phones, computers and other devices', fearing they might be compromised.'[265] Consequently, while President Putin is known to be extremely technologically cautious, his reticence, itself a KGB legacy, seemingly permeates the Kremlin's inner circle. [266]

But even if hacking does not provide concrete evidence that a person might be disaffected or open to recruitment, it may offer at least some degree of insight into their day-to-day affairs. In 2019, members of Russia's political and business elite were

testimony/deputy-director-cohen-delivers-remarks-on-cia-of-the-future-at-cornell-university.html [accessed 1 January 2018].

[262] Surveillance Self-Defense (30 October 2015) The problem with mobile phones. Available at: https://ssd.eff.org/en/module/problem-mobile-phones [accessed 1 January 2018].

[263] Ibid.

[264] Judah, B. (19 October 2014) Putin's coup: How the Russian leader used the Ukraine crisis to consolidate his dictatorship, *Politico*. Available at: https://www.politico.com/magazine/story/2014/10/vladimir-putins-coup-112025_full.html#.WJo84H9yXE9 [accessed 1 March 2018].

[265] Miller, G. (14 September 2016) As Russia reasserts itself, U.S. intelligence agencies focus anew on the Kremlin, *The Washington Post.* Available at: https://www.washingtonpost.com/world/national-security/as-russia-reasserts-itself-us-intelligence-agencies-focus-anew-on-the-kremlin/2016/09/14/cc212c62-78f0-11e6-ac8e-cf8e0dd91dc7_story.html?postshare=371473956824384&tid=ss_tw-bottom&utm_term=.d8941ad4f02e#comments [accessed 31 November 2017].

[266] Shuster, S. (24 March 2014) Putin's fear of texting kept U.S. spymasters in the dark, *Time*. Available at: http://time.com/35932/ukraine-russia-putin-spies-kgb/ [accessed 10 January 2018].

exposed in a cache of hacked documents known as the "Dark Side of the Kremlin".[267] Openly published by a group of Eastern European 'hacktivists', the materials exposed over one hundred gigabytes of personal data from Kremlin officials, arms dealers, oligarchs, and defence personnel, offering, as Bellingcat specialists told *Foreign Policy*, a unique glimpse into Russian affairs: "[the] Russian [hacks] that have had the most consequences are more internal palace politics—the FSB hacking someone to embarrass them".[268] It underscores that even Russia's most powerful elite are not invulnerable to hacking, often due to incompetence; *Meduza* reported in 2017 how Russian politicians' correspondences were being hacked due to shoddy security practices by individual officials, with victims using insecure instant messengers when discussing sensitive affairs, rather than the government encrypted RSNet email system.[269] However, besides showing that officials had been targeted by the FSB for potential blackmail purposes (possibly encouraging greater caution in the future) the disclosures were largely non scandalous, meaning if officials were disaffected they clearly left little digital evidence.[270] Thus, while it shows that Russian officials are not immune to hacking, it also illustrates that the gains to be made, especially against those in more sensitive positions, are more likely limited, placing greater onus on the need for trust before hacking's risks are undertaken.

[267] Mackinnon, A. (28 January 2019) Hackers turn the tables on Russia, *Foreign Policy.* Available at: https://foreignpolicy.com/2019/01/28/hackers-turn-the-tables-on-russia-hacking-leaking-cyber-documents-wikileaks/ [accessed 19 March 2019].
[268] Ibid.
[269] Meduza (19 July 2017) Moscow's cyber-defense: how the Russian government plans to protect the country from the coming cyberwar. Available at: https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense [accessed 15 March 2017].
[270] Mackinnon, A. (28 January 2019) Hackers turn the tables on Russia, *Foreign Policy.* Available at: https://foreignpolicy.com/2019/01/28/hackers-turn-the-tables-on-russia-hacking-leaking-cyber-documents-wikileaks/ [accessed 19 March 2019].

Evaluation

This chapter began by examining the notion that agents might be cultivated through online social communications. Cyberspace's increasingly popular social channels, comprised of billions of users, generate such enormous amounts of noise that even the most invasive surveillance states struggle to keep pace. As such, it is possible, in ideal conditions, for intelligence officers to pursue their quarry online, building seemingly innocent connections through messages hidden in plain sight. The fact that Russian and Chinese intelligence officers have targeted thousands of foreign officials through professional networks, such as LinkedIn, underscores just how difficult it can be for counterintelligence to monitor these spaces. Similarly, the US intelligence community's dependency on "deconfliction" groups to avoid overlap between its myriad of operations in online video games, exemplifies how practically any form of online social bonding offers serious recruitment opportunities.

However, while incriminating communications may, in most cases, be lost in the noise, intelligence officers cannot guarantee that their social communications, especially those sent to sources who reside in hard target states, will remain concealed forever. Both Russia and China have established the legal and technical foundations to vastly expand their Internet surveillance prowess. Through wide reaching and stringently applied data-localisation laws, both governments have compelled mainstream telecommunications and Internet companies to either cooperate with the state, or face national level restrictions. Those who comply, as a consequence, must cede their customers' communication data, including content and metadata, at the behest of the authorities, squandering notions of privacy while delegitimising the growing norm of social encryption. Any social communication sent through Russian and Chinese Internet infrastructure is thus inherently vulnerable, and could theoretically

expose agents long after their initial recruitment.

The safest recruitment efforts will succeed not because of their dependence on social communications, but rather because of its avoidance. Without a means to conceal their incriminating connections, and out of concern of drawing further scrutiny from counterintelligence, operatives will more than likely want to steer clear of social communications in cyberspace. However, since they cannot openly instruct their targets without revealing their intelligence officials, and thus alarming the target, they are increasingly dependent on their target's own sensibilities. The person being recruited must recognise that their online relationships are inherently insecure, and forgo any overzealous contact. Fortunately for Western operatives, many Russian and Chinese Internet users understand the scope of domestic surveillance, and adjust their behaviour accordingly, but these spaces should not be used unless there is sufficient confidence that the target will take necessary precautions.

Similar issues occur for those who wish to volunteer their services. Although official websites offer a direct link to intelligence agencies, these spaces rank as priority targets for foreign surveillance. And while governments cannot necessarily see the content of any communications sent, the mere notion that a Russian or Chinese official, especially one with access to classified information, had connected to these websites, would likely draw counterintelligence's interest. As such, the onus is on the volunteer to take the chance and use security precautions. However, since these websites offer an ideal platform for counterintelligence to waste their opponent's time and resources, or even entrap them with dangles, intelligence officers will likely want proof of a secure and valid approach. Thus, not only must the volunteer be sensible enough to connect to these websites safely, but they must also be willing to send highly incriminating bona fides through potentially vulnerable means, thereby confirming that they have good

access to valuable intelligence. And with mounting risks in hard target conditions, as personified by Langley's decision to discourage Russian volunteers from contacting its website, many are likely to be discouraged.

Given these challenges, a great deal of operational effort can be spared by running surveillance against prospective spies. While the traditional practice of bugging a target's premises with hidden listening devices remains exceedingly dangerous, it is far from the only electronic option available. Through gathering operational data in cyberspace, intelligence officers can identify those with access to secrets, and select the path of least resistance to their recruitment. One of the simplest resources at the operative's disposal is social media, in the sense that millions of online users share a great deal about themselves in full public view. Social and professional networks, as personified by Facebook and LinkedIn, contain masses of personal and professional information, offering insights into a person's potential access to classified information, their susceptibility to a recruitment pitch, or whether they often travel to a particularly safe location for a personal meeting. Risks, however, start to mount if the person-of-interest applies privacy settings, restricting their public networks to 'friends' only. To access this data, operatives would need to be invited into their networks, openly advertising their connection to security services.

Alternatively, hacking can grant access to enormous repositories of personal information. As exemplified by the OPM case, many government and private sector organisations store vast amounts of personal data, ranging from sensitive vetting forms, to credit card information, medical bills, online activities, or even infidelities. But while the US intelligence community would have a great deal to gain by achieving an OPM-esque breach of its own, these largescale databases boast robust cyber defences. Both Russia and China have introduced broad ranging legislation to tighten their defences,

forcing the private sector to sufficiently protect their customers' data. Thus, although they are not rendered unfeasible, the costs pursuant to a largescale breach continue to rise. In many cases, a breach can only realistically be achieved with the aid of insiders who know the relevant encryption keys, and even in these instances, security practices such as multifactor authorisation or the 'two person rule' mean that a single source may not actually be sufficient. Those factors, combined with the potential political fallout of a largescale breach, vastly increase the potential risks.

As opposed to hacking heavily defended databases, intelligence agencies can also pursue individual devices. A person-of-interest's phone, laptop, or even smart television can provide an invaluable window into their personal affairs. The inbuilt microphones and cameras of a modern smartphone can even follow targets wherever they travel, offering a mobile surveillance platform. But hacking of this kind is not without its own risks. In today's vibrant cybersecurity market, finding an effective entry point into a personal device is a high cost endeavour, as exemplified by the millions of dollars charged for so-called 'zero day' exploits. And while solutions exist, including social engineering or "close access" bugging, there is no outright risk-free approach. Breaking into a target's hotel or apartment to surreptitiously plant malware clearly entails abundant risks, but socially engineering someone to infect their own device only works if the victim is duped by the ruse.

As such, the risks inherent in surveillance must be weighed against the probabilities of reward. Although these pathways can yield a great amount about a person's day to day affairs, there is no guarantee that open sources or hacking will reveal anything of exceptional recruitment value. Indeed, both Russia and China have implemented stringent rules to ensure that those in sensitive positions refrain from oversharing in cyberspace, while even personal devices have become symbols of fear

against rampant government eavesdropping. This, in turn, decreases the likelihood that something of meaningful recruitment value will be learned. The claim that Kremlin officials remove their phone batteries before discussing sensitive matters, out of fear that their surveilled indiscretions may land them in the next round of purges, only reinforces this point. Again, this pushes up the need for confidence in the target's behaviour, to determine a person's proclivity for indiscretion or oversharing, ensuring that these costly risks or not taken unnecessarily.

Consequently, the picture painted here is far from optimistic. Cyberspace certainly opens some doors in both recruitment and surveillance, but these are constricted by rapidly rising risks. Thus, despite the enthusiastic assumptions presented by scholars in the literature review, these do not translate into hard target conditions. The fundamental problem is that cyber-enabled tradecraft in both functions requires a high degree of trust in the prospective spy's behaviour, and yet, that trust is increasingly difficult to build in surveilled cities. Therefore, it is clear that, at this stage, cyberspace leans heavily toward pessimism.

Chapter 6
Cyber-enabled handling & collection

Introduction

The next stage is to test this dissertation's hypothesis in *handling* and *collection.* It begins by examining the feasibility of covert communications within the confines of a heavily surveilled Internet. Building on key assumptions from the literature review, it first assesses the prospects of common off-the-shelf solutions, including anonymising tools such as The Onion Router and Virtual Private Networks. This serves two purposes, first by showing how off-the-shelf systems offer only limited security inside Russia and China, and second, by revealing the conditions any covert communication system would need to achieve to remain secure. Its central premise is to show that a system only works if its connections can be hidden in plain sight, but since Russia and China maintain tight control over Internet activity, any secure system with notably irregular traffic is increasingly likely to draw scrutiny. This, consequently, pushes up the need for more costly communication tools, thus increasing the need for trust in the agent's willingness to use the equipment at their disposal, and to do so responsibly.

In the next stage, the focus is narrowed to the agent's ability to acquire the secrets that they have been tasked to collect. It focuses on the shift from paper based to electronic documents, which opens a new array of possibilities for accessing and storing classified information. Its first argument is that while largescale breaches are unlikely to be feasible within heavily monitored networks, agents could nonetheless extract small amounts of information through microelectronic storage devices or even automate the collection process by uploading advance malware toolkits. In both instances, it will be argued that through the emergence of tighter network controls, stronger cybersecurity, and the monitoring of employee behaviour, the risks of illicit

exfiltration are rapidly rising. Hence, the chapter shows that collection is equally reliant on trust in the agent's behaviour.

Handling

At this stage of the relationship, the agent is officially brought into the fold, meaning covert communication systems can be applied and security precautions initiated. It is important to reiterate that even recruited agents must, from time to time, meet their handlers face-to-face.[1] Personal meetings offer an invaluable means to develop trust between the parties, stave off doubts, and provide a much needed boost of morale.[2] However, impersonal communications allow handlers to stay abreast of their agents wellbeing, offer tasking and direction, and receive their take.

Many of the classic methods from the Cold War remain in use, but retain their original insecurities. This was personified in 2014, when Moscow agent Yevgeny Chistov was arrested by the FSB due to serious flaws in his tradecraft.[3] First, Yevgeny's CIA liaison officer was observed mailing an "undercover letter" to his address, rousing the security service's interest.[4] Then, when surveillance identified dead-drops containing money and messages, one was observed at the point when Yevgeny removed its contents, confirming the FSB's suspicions and leading to the arrest of the agent shortly after.[5] Alternatively, more secure systems, including SRAC, have seen some upgrades in the digital era, but they retain many of their original issues.

[1] Gioe, D. V. 'The more things change': HUMINT in the cyber age', in *The Palgrave Handbook of Security, Risk and Intelligence*, edited by Robert Dover, Huw Dylan, and Michael Goodman (London, Palgrave, Macmillan, 2017), p. 221-222.
[2] Ibid.
[3] Meduza (31 July 2019) 'I'd be willing to work against this government with Satan himself' We talked to a suburban Russian policeman who spied for the CIA, fought in eastern Ukraine, and got sentence to 13 years for treason. Available at: https://meduza.io/en/feature/2019/07/31/i-d-be-willing-to-work-against-this-government-with-satan-himself [accessed 15 September 2020].
[4] Ibid.
[5] Ibid.

Former SIS officer Richard Tomlinson wrote about an evolved form of SRAC in 2001, which bore heavy resemblance to its Cold War predecessor:

> The agent writes a message on a laptop computer, then downloads it into the SRAC transmitter, a small box the size of a cigarette packet. The receiver is usually mounted in the British embassy and continually sends out a low-power interrogation signal. When the agent is close enough, in his car or on foot, his transmitter is triggered and transmits the message in a high-speed burst of VHF.
>
> The transmitter is disguised as an innocuous object and for many years 'Garfield Cat' stuffed animals were popular as their sucker feet allowed the agent to stick the transmitter on the side window of his car, giving an extra clear signal as he drove past the embassy.[6]

Further signs of evolution emerged in 2007, when Russian media released compromising pictures of SIS officers handling a digital 'spy-rock'.[7] The artificial rock, that was hidden among other rocks in a Moscow park, contained an electronic transmitter allowing intelligence officers and their agents to relay communications from a considerable distance.[8] The agent 'would walk past and press a button on a hand-held electronic device to transfer information', before an SIS operative later downloaded the data 'with his own device'.[9] With the rock, the agent could remotely upload their message at a time of their choosing, to be downloaded by intelligence officers days later.[10] And although the rock was portrayed by headlines as an example of twenty-first century espionage, in actuality it worked exactly the same as the SRAC embassy receiving units used three decades earlier.

However, the sending of electronic messages over short distances, whether transmitted to an embassy base station or to a spy rock in a Moscow park, is still

[6] Tomlinson, R. *The big breach: from top secret to maximum security*, (Edinburgh, Cutting Edge, 2001), p. 69.
[7] Roxburgh, A. *Strongman: Vladimir Putin and the struggle for Russia*, (London, I.B. Tauris, 2012), p. 149.
[8] Ibid.
[9] Corera, G. *The art of betrayal: life and death in the British secret service*, [Kindle version] (London, Weidenfeld & Nicolson, 2011). Accessed 15 March 2020, p. 397.
[10] Roxburgh, A. *Strongman*, p. 149.

vulnerable to eavesdropping. If counterintelligence can determine where a transmission is likely to occur (such as by monitoring operatives), then sophisticated listening equipment could be deployed nearby to detect and triangulate any agents trying to send a message. Anna Chapman, of Russia's 2010 Illegal Ring, experienced this problem first-hand.[11] While supposedly relaxing inside New York's cafes and bookstores, Chapman would secretly send burst transmissions, akin to SRAC, from her laptop to her Russian handler sitting in a minivan across the street, creating what the FBI described as an 'ad hoc' network.[12] But the FBI, ready with listening equipment positioned in the nearby vicinity, detected these transmissions and used them as evidence against Chapman in court.[13] Although it remains unclear just how effective FBI technical countermeasures were against this localised network, ensuing criminal reports hinted at a great deal of success:

> … the Americans may not have succeeded in intercepting and decoding everything sent from Ms Chapman's laptop. But the Russians cannot be sure. If burst transmissions over ad-hoc networks between nearby laptops are hard to monitor then it would be a neat counter-measure to mention them frequently in the criminal complaint. It will be a bold Russian spy who includes them in operational planning in future.[14]

Similar issues likely arose with SIS's spy rock. The fact that SIS officers were covertly photographed while tending to the rock implies that the FSB knew about its location for some time, as Tony Blair's chief of staff lamented five years later, they were caught "bang to rights".[15] It would not be a leap if, knowing the rock's location, FSB surveillance teams had surrounded the vicinity with technical listening equipment, to

[11] Warner, M. *The rise and fall of intelligence: an international security history*, [Kindle version] (Washington, Georgetown University Press, 2014). Accessed 21 January 2020, p. 301-302.
[12] Ibid.
[13] Lucas, E. *Deception: Spies, lies, and how Russia dupes the West*, (London, Bloomsbury Publishing PLC, 2013), p. 144.
[14] Ibid.
[15] BBC News (19 January 2012) UK spied on Russians with fake rock. Available at: https://www.bbc.co.uk/news/world-europe-16614209 [accessed 18 January 2021].

find anyone transmitting nearby. And in fact, the victim of Salisbury's 2018 Novichok poisoning, Sergei Skripal, was allegedly observed by security officers while trying to transmit to a British spy rock in a Moscow park (in an investigation that spanned from 2004-2006).[16]

Figure 1: SIS officers observed removing the 'spy rock' by FSB surveillance teams.[17]

Another digitally upgraded legacy from the Cold War is satellite uplink. Today, encrypted satellite communications, specifically satellite phones, have evolved well beyond military and intelligence circles, playing key roles in fields such as journalism,

[16] Evans, M. (5 March 2018) Sergei Skripal: the 'spy with the Louis Vuitton bag' allegedly poisoned during retirement in Salisbury, *The Telegraph.* Available at: https://www.telegraph.co.uk/news/2018/03/05/sergei-skripalthe-spy-louis-vuitton-bag-allegedly-poisoned-quiet/ [accessed 13 October 2020].

[17] The Sun (19 January 2012) UK admits using fake rock to spy. Available at: https://www.thesun.co.uk/archives/news/314694/uk-admits-using-fake-rock-to-spy/ [accessed 20 October 2020].

business, and maritime shipping.[18] However satellite phones are heavily restricted in certain countries, including Russia and China, where satellite phone owners are legally obliged to purchase special SIM cards that can be monitored by security services.[19] Moreover, with modern detection capabilities, illicit satellite broadcasts have proven vulnerable to detection and triangulation, leading to repeated arrests of suspected spies in various parts of the world, and to the targeted bombing of journalists and dissidents in warzones such as Syria.[20] In 2012, a contractor named Alan Gross was arrested for smuggling a specialised SIM card to pro-democracy activists in Havana, one designed to 'keep satellite phone transmissions from being pinpointed within 250 miles'.[21] Gross is accused of trying to establish illicit satellite communications for Cuban dissidents, through a US government programme called USAID.[22] But the SIM card, which according to US officials was not available on the open market and reserved for use by the CIA and DoD, was discovered during his arrest.[23] Although it is unclear whether the Cubans were able to a develop a countermeasure, or whether the system remains secure against sophisticated counterintelligence actors, it *is* clear that its discovery was highly incriminating for Gross.

[18] Committee to Protect Journalists (24 February 2012) Caveat utilitor: Satellite phones can always be tracked. Available at: https://cpj.org/2012/02/caveat-utilitor-satellite-phones-can-always-be-tra/ [accessed 23 July 2020].
[19] Telestial (8 November 2017) Countries where satellite phones are banned or restricted. Available at: https://blog.telestial.com/2017/11/countries-where-satellite-phones-banned-or-restricted/ [accessed 1 January 2018]
[20] Shachtman, N. (29 June 2010) FBI: spies hid secret messages on public websites, *Wired*. Available at: https://www.wired.com/2010/06/alleged-spies-hid-secret-messages-on-public-websites/ [accessed 23 June 2016]; BBC News (22 March 2010) Biofuel bus driver fined over sat phone use in India. Available at: http://news.bbc.co.uk/1/hi/england/london/8579614.stm [accessed 20 February 2018]; Committee to Protect Journalists (24 February 2012) Caveat utilitor: satellite phones can always be traced. Available at: https://cpj.org/blog/2012/02/caveat-utilitor-satellite-phones-can-always-be-tra.php [accessed 20 February 2018];.
[21] Bloomberg (12 February 2012) AP impact: USAID contractor work in Cuba detailed. Available at: http://www.businessweek.com/ap/financialnews/D9SSHGPG2.htm [accessed 12 March 2018].
[22] Ibid.
[23] Rogers, K. (1 May 2015) Why was Alan Gross smuggling satellite phones into Cuba?, *Vice*. Available at: https://www.vice.com/en/article/4x379w/why-was-alan-gross-smuggling-satellite-phones-into-cuba [accessed 12 August 2020].

As opposed to short range or satellite transmissions, it may be possible to communicate covertly in cyberspace. In 2017, the NSA drew attention for sending seemingly innocuous 'tweets' to its global audience, which were actually signals for a Russian asset.[24] By sending tweets from its official account such as "Samuel Morse patented the telegraph 177 years ago. Did you know you can still send telegrams? Faster than post & pay only if it's delivered", the NSA was proving to their new asset that he was genuinely working with US intelligence *and* confirming its willingness to continue the operation.[25]

But sending one-way signals is not the same as a frank and open two-way conversation, and herein complications arise. Over time, various rudimentary systems have come to light offering what, on paper, offers at least some semblance of security. Former CIA chief, David Petraeus, inadvertently drew public interest in 2012 for his use of the so-called 'email dead-drop'.[26] This technique entailed storing unsent messages in the draft email folder of an account shared with his biographer, turned mistress, Paula Bradwell, meaning they could read each other's messages without actually sending any communications.[27] Alternatively, judiciously sending emails from commercial providers seems to have sufficed in some instances. When CIA operative, Ryan Fogle, was apprehended by FSB officers in Moscow in 2013, the Russians revealed a letter carried for his-would be source, detailing instructions on how to continue contact through Google's Gmail:

Dear friend,

[24] Business Insider (13 February 2018) The NSA sent coded messages to a shadow Russian on its official Twitter account. Available at: https://www.businessinsider.com/nsa-sent-coded-messages-to-russian-using-its-official-twitter-account-2018-2?r=US&IR=T [accessed 14 March 2019].
[25] Ibid.
[26] Slate (13 November 2012) Instead of "dead dropping" Petraeus and Broadwell should have used these email security tricks. Available at: https://slate.com/technology/2012/11/petraeus-and-broadwell-should-have-used-pgp-encryption-and-tor-not-dead-dropping-to-secure-affair-emails.html [accessed 16 July 2017].
[27] Ibid.

This is an advance from someone who is very impressed by your professionalism and who would greatly value working together with you in the future. For us, your safety is of the utmost importance, so we have chosen this route to make contact with you. And we will continue to take steps to secure your safety and keep our correspondence secret.

We are prepared to offer you $100,000 and discuss your experience, expertise and cooperation, and your payment might be far greater if you are prepared to answer some specific questions. Additionally, for long-term cooperation we offer up to $1,000,000 a year with the promise of additional bonuses for information that will help us.

To contact us again, please open a new Gmail account, which you will use only for communicating with us, in an internet café or a café with a WiFi connection. When signing up, do not use any personal information that could be used to identify you and the new account. So do not offer any real contact information, i.e. your telephone numbers or other email addresses.

If Gmail asks for your personal information, please, start the registration process again and try not to give them any information. After you register the new inbox, send an email to the address unbacggdA(at)gmail.com, and then check the inbox again exactly one week later to see if you have received our reply.

If you register the new email account in a café with a netbook or another device (for example, a tablet), then please do not use your own device with your own personal data on it. If possible, you should get a new device to connect with us, for cash. We will reimburse you for the purchase.

Thank you for reading this. We eagerly await the possibility of working with you in the near future.

Your friends.[28]

While the letter's authenticity is open to doubt, these instructions were surprising for their simplicity, '[accounts] on Google's Gmail? Was this the new face of spying?'.[29] However, it is worth considering Russia's limited surveillance powers at the time. As discussed in chapter 5, prior to the introduction of sweeping surveillance laws and the expansion of SORM, the FSB were unable to access the servers of mainstream Internet

[28] The Telegraph (14 May 2013) CIA agent 'detained in Moscow': his 'letter' in full. Available at: http://www.telegraph.co.uk/news/worldnews/europe/russia/10056972/CIA-agent-detained-in-Moscow-his-letter-in-full.html [accessed 16 July 2017].
[29] Grey, S. *The new spymasters: inside espionage from the Cold War to global terror,* (New York, Viking, 2015), p. 272.

companies.[30] But with the expansion of its powers, today the FSB would face few problems accessing the Gmail accounts of Russian citizens, including accessing any messages sent and the contents of their draft folders. Agents could opt for an email provider which cannot be easily accessed by surveillance, but questions might arise as to why someone privy to classified information was sending messages abroad via an email account that cannot be monitored by the state.

With growing demand for online privacy by a wide range of actors ranging from activists to law enforcement, many security specialists advocate the use of tools which reroute and effectively anonymise Internet traffic.[31] There are two commonly advocated and widely used approaches, Virtual Private Networks (VPNs), or The Onion Router (Tor), both of which function as proxy networks, meaning surveillance cannot see what happens within these networks.[32] This offers two advantages, first the user can access content that is otherwise blocked by national filters, and second, they can send communications with some degree of privacy. To surveillance, connections to a website, such as a reliable email provider, would appear to originate from an IP address registered with the proxy, despite the fact it is merely rerouting traffic on behalf of its customers.[33] Resultantly, as one former CIA officer contends, tools such as Tor offer the prospect of 'secure links with real time connectivity', and may amount to 'nothing short of a tradecraft revolution'.[34]

---

[30] Lowenthal, M. *Intelligence: From secrets to policy*, [Kindle version], (Thousand Oaks, CQ Press, 2017). Accessed 30 February 2017, see chapter 17.
[31] FrontLine - Digital security and privacy for human rights defenders. Available at: https://www.frontlinedefenders.org/en/digital-security-resources [accessed 23 June 2017], p. 51-55; Security in-a-box - Remain anonymous and bypass censorship on the Internet. Available at: https://securityinabox.org/en/guide/anonymity-and-circumvention/ [accessed 22 December 2018]; Quartz (6 April 2015) How the New York Times is eluding censors in China. Available at: https://qz.com/374299/how-the-new-york-times-is-eluding-chinas-censors/ [accessed 23 June 2017].
[32] Security In-a-Box - Remain anonymous and bypass censorship on the Internet. Available at: https://securityinabox.org/en/guide/anonymity-and-circumvention/ [accessed 23 July 2020].
[33] Ibid.
[34] Gioe, D. V. 'The more things change', p. 220.

VPNs reroute traffic through a single, encrypted, high-bandwidth relay, which means that the provider can see the IP addresses and the websites browsed of anyone connected to their networks.[35] By contrast, Tor reroutes traffic through a series of globally dispersed, encrypted, and independently run relays, and was originally designed by the US government (albeit it is now privately operated) for military and intelligence affairs, as DARPA research papers show:

> The primary goal of Onion Routing is to provide private, traffic analysis resistant communications over a public network at reasonable cost and efficiency. Communications are intended to be private in the sense that both the public network itself and any eavesdropper on the network cannot determine the contents of messages flowing from Alice and Bob, and she cannot tell that Alice and Bob are communicating with each other.
>
> A secondary goal is to provide anonymity to the sender and receiver, so that Alice may receive messages but be unable to identify the sender, even though she may be able to reply to those messages. For example, open source intelligence gathering via the web and pseudonym based email communications that hide the true identities of both sender and receiver.[36]

There are thousands of these relays operated by independent users around the world, three of which are automatically selected every time a person connects to the network.[37] If one node is compromised, Tor would only reveal the IP address of the previous node, meaning surveillance would need to control all three nodes to sufficiently de-anonymise Tor users.[38] Its decentralised system means that no single entity has a controlling monopoly over its relays, thus even Tor's developers are unable to de-anonymise their users.[39] Unfortunately, because these relays are globally dispersed and independently maintained, Tor's higher degree of security more often comes at the

[35] Kizza, J. M. *Guide to computer network security: fourth edition,* (New York, Springer, 2017), p. 391.
[36] Reed, M. G. & Syverson, P. F. 'Onion routing', *Center for High Assurance Computer Systems, Naval Research Laboratory,* 1999.
[37] The Conversation (20 March 2017) Tor upgrades to make anonymous publishing safer. Available at: https://theconversation.com/tor-upgrades-to-make-anonymous-publishing-safer-73641 [accessed 23 July 2020].
[38] Security In-a-Box - Tor browser for Windows – online anonymity and censorship circumvention. Available at: https://securityinabox.org/en/guide/torbrowser/windows/ [accessed 23 July 2020].
[39] Ibid.

expense of a much slower bandwidth speed.[40]

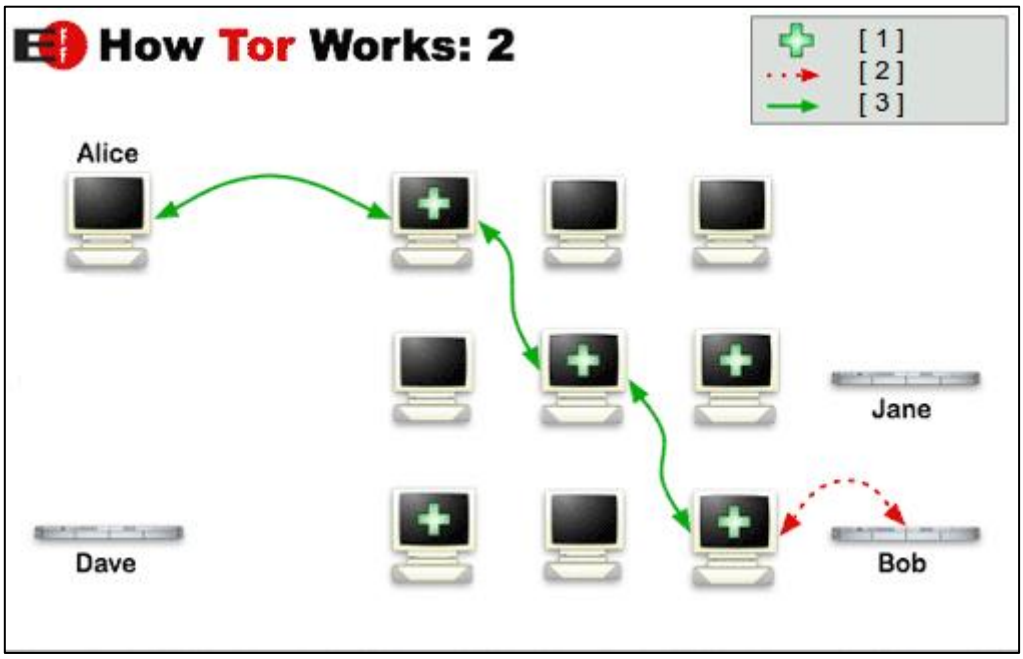

Figure 2: Diagram of Tor's relay system.[41]

Furthermore, the popularity of services such as Tor and VPN creates an enormous amount of traffic within which malicious actors, including intelligence officers and their agents, can blend. By 2014 alone, almost half a billion people were using VPN services in some capacity, a number that has since risen to around one quarter of the world's population.[42] Moreover, while VPNs are often used for pernicious purposes, such as hacking or Internet piracy, they are also commonly used to access restricted content. For example, tourists, business workers, and even citizens in China commonly use VPNs to circumvent the Great Firewall and access Western social

[40] Security In-a-Box - Remain anonymous and bypass censorship on the Internet. Available at: https://securityinabox.org/en/guide/anonymity-and-circumvention/ [accessed 23 July 2020].
[41] Tor - Tor: overview. Available at: https://2019.www.torproject.org/about/overview.html.en [accessed 20 October 2020].
[42] Digiday (18 November 2014) Seriously dark traffic: 500 mil. People globally hide their IP addresses. Available at: https://digiday.com/uk/vpn-hide-ip-address-distort-analytics/ [accessed 21 March 2020]; Statista (22 July 2019) Global VPN usage reach 2018, by region. Available at: https://www.statista.com/statistics/306955/vpn-proxy-server-use-worldwide-by-region/ [accessed 21 March 2020].

media.[43] By comparison, Tor tends to attract a smaller, more security-conscious audience of around a few million users.[44] Tor also opens access to a vast array of otherwise hidden websites collectively known as the dark web, an internet black-market which facilitates a wide range of serious crime.[45] In 2014, a study claimed that eighty percent of Tor activity was used for paedophilia.[46] Similarly, a single dark web narcotics trading website, known as the Silk Road, acquired over $1 billion worth of drug sales in a mere two years (2011 to 2013) before its founder, Ross Ulbricht, was arrested by the FBI.[47]

But because VPNs and Tor help to circumvent government controls and facilitate serious crime, they have become increasingly tempting targets for Western and authoritarian states alike. For instance, governments use technical filtering systems such as 'deep packet inspection' (DPI) to identify and block VPN or Tor traffic.[48] Deep packet inspection is commonly used by most developed states on an ad hoc basis, however some regimes apply it on a national scale.[49] In 2014, Russia connected DPI technologies with the SORM black boxes mandatorily installed throughout its Internet companies and telecommunications providers. As such, '[the] two most intrusive

[43] Li, E. (6 July 2017) For many Chinese Internet users, it's time to get a new VPN, *South China Morning Post*. Available at: https://www.scmp.com/news/china/policies-politics/article/2101435/many-chinese-internet-users-its-time-get-new-vpn [accessed 23 July 2020].
[44] Tor - Users. Available at: https://metrics.torproject.org/userstats-relay-country.html [accessed 22 September 2020].
[45] FBI (` November 2016) A primer on DarkNet marketplaces: what they are and what law enforcement is doing to combat them. Available at: https://www.fbi.gov/news/stories/a-primer-on-darknet-marketplaces [accessed 22 September 2020].
[46] Greenberg, A. (30 December 2014) Over 80 percent of dark-web visits relate to paedophilia, study finds, *Wired*. Available at: https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/ [accessed 23 July 2020].
[47] Bearman, J. et al. (May 2015) The rise and fall of Silk Road: how a 29-year-old idealist built a global drug bazaar and became a murderous kingpin, *Wired*. Available at: https://www.wired.com/2015/04/silk-road-1/ [accessed 14 July 2017].
[48] Paul, K. (18 February 2015) Russia wants to block Tor, but it probably can't, *Vice*. Available at: https://www.vice.com/en_us/article/ypwevy/russia-wants-to-block-tor-but-it-probably-cant [accessed 23 July 2020]; TechNode (17 March 2016) Behind the scenes: here's why your VPN is down in China. Available at: https://technode.com/2016/03/17/behind-scenes-heres-vpn/ [accessed 20 November 2017].
[49] Soldatov, A. & Borogan, I. *The red web: the struggle between Russia's digital dictators and the new online revolutionaries*, [Kindle version] (New York, Public Affairs, 2015). Accessed 1 January 2018, see chapter 8.

surveillance technologies were finally combined, to be used by the Russian security services all over the country.'[50] And with DPI, authorities can force VPN providers to either cooperate with the state or face national blocking, as was demonstrated in 2017, when after years of ad hoc restrictions, China ordered telecommunications companies to block almost all illicit VPN traffic within one year.[51] The impact was wide reaching, Apple alone blocked over 674 VPN products from its regional online store.[52] Similarly, Russia's new Anti-VPN law, which entered force in November 2017, threatens to block any VPN provider who refuses to surrender their customers' personal information to the government.[53]

Some services do remain, often by simply cooperating with the state. Studies have identified connections between almost half of the world's most popular VPN providers and the Chinese government, indicating that major services may be sharing their customers' data with the authorities in exchange for access to the Chinese market.[54] As the researchers' discovered, several mainstream VPN providers boasted limited privacy policies, and were either legally based in China or owned by Chinese companies, exposing them to the full weight of Chinese surveillance laws.[55] Alternatively, VPN providers can try to obfuscate their traffic to frustrate detection

[50] Ibid, see chapters 8 & 10.
[51] Xiao Qiang, a specialist in China censorship, told *The Guardian* "[this] is a significantly escalated form of Internet control and shows there is unprecedented urgency and desperation at the top of the government … This is clearly about the highest levels of political struggle and the different factions using the Internet as their battlefield", he added "[there] have always been controls, but this will be another level." For more details, see Haas, B. (11 July 2017) China moves to block internet VPNs from 2018, *The Guardian.* Available at: https://www.theguardian.com/world/2017/jul/11/china-moves-to-block-internet-vpns-from-2018 [accessed 11 January 2018].
[52] Bradshaw, T. (21 November 2017) Apple drops hundreds of VPN apps at Beijing's request, *Financial Times.* Available at: https://www.ft.com/content/ad42e536-cf36-11e7-b781-794ce08b24dc [accessed 25 November 2017].
[53] BBC News (1 November 2017) Explainer: What is Russia's new VPN law all about? Available at: http://www.bbc.co.uk/news/technology-41829726 [accessed 31 January 2018].
[54] Murgia, M. (22 November 2018) Study finds half of most popular VPN apps linked to China, *Financial Times.* Available at: https://www.ft.com/content/e5567d8a-ee65-11e8-89c8-d36339d835c0 [accessed 25 November 2018].
[55] Ibid.

capabilities, but, due to the fact that DPI capabilities are constantly adapting, there is no guarantee they will remain hidden forever.[56] Unable to force Tor's developers to hand over their customers' data, China has opted for simply banning Tor traffic, forcing its developers into constant conflict with state surveillance.[57] Normally, Tor's relays are publicly disclosed, but constant pressure from China's filters has increased dependency on unique hidden relays, or 'secret bridges', which are harder to detect but also aggressively pursued by Chinese surveillance.[58] By 2012 China could allegedly detect and close down some unpublished relays in a matter of minutes.[59] Various techniques have since developed to mask Tor traffic in China, with varying levels of success (some bridges even remain active for several months), however the fact remains that stable connections for Chinese users rarely last.[60] This is best illustrated by Tor's relatively small Chinese usership, of around 3000 active users, which is strikingly meagre when compared to Russia's 200,000 strong Tor community.[61]

Moreover, proxies are not altogether impenetrable, with the targeted hacking of VPN providers raising concerns that the identities and activities of customers could be

[56] Meduza (10 April 2019) Russia's censorship agency has threatened to block OpenVPN. At worst, that move could interfere with systems from banking to cell service. Available at: https://meduza.io/en/feature/2019/04/10/russia-s-censorship-agency-has-threatened-to-block-openvpn-at-worst-that-move-could-intefere-with-systems-from-banking-to-cell-service [accessed 18 January 2020].
[57] Paul, K. (18 February 2015) Russia wants to block Tor, but it probably can't, *Vice.* Available at: https://www.vice.com/en_us/article/ypwevy/russia-wants-to-block-tor-but-it-probably-cant [accessed 23 July 2020].
[58] MIT Technology Review (4 April 2012) How China blocks the Tor anonymity network. Available at: https://www.technologyreview.com/2012/04/04/186902/how-china-blocks-the-tor-anonymity-network/ [accessed 20 September 2020].
[59]Winter, L. & Lindskog, S. 'How the Great Firewall of China is blocking Tor', *2nd USENIX Workshop on Free and Open Communications on the Internet,* 2012, p. 5.
[60] Medium (4 October 2019) Using Tor in China. Available at: https://medium.com/@phoebecross/using-tor-in-china-1b84349925da [accessed 20 September 2020].
[61] Tor Metrics – Russia Users 2017-01-01 to 2018-01-01. Available at: https://metrics.torproject.org/userstats-relay-country.html?start=2017-01-01&end=2018-11-11&country=ru&events=off [accessed 1 February 2019]; Tor Metrics – China Users 2017-01-01 to 2018-01-01. Available at: https://metrics.torproject.org/userstats-relay-country.html?start=2017-01-01&end=2018-01-01&country=cn&events=off [accessed 1 February 2019].

compromised.[62] In 2020, around 1.2 terabytes worth of customer data, including user passwords, personal information, and lists of websites visited, was leaked onto the Internet, all of which pertained to VPN providers who claimed not to store customer data.[63] By comparison, Tor's criminal advantages have made it a tempting target for intelligence powers, as underscored by a 2012 NSA presentation titled 'Tor Stinks'.[64] On the one hand, the presentation, disclosed by Snowden, revealed Fort Meade's struggle to de-anonymise Tor users on a large scale:

> [we] will never be able to de-anonymize all Tor users all the time. With manual analysis we can de-anonymize a very small fraction of Tor users,', adding, importantly 'however, no success de-anonymizing a user in response to a TOP [target office of primary interest] request / on demand.[65]

On the other hand, it also showed that the NSA intended to expand its access to Tor relays in conjunction with GCHQ, albeit its success in this regard remains unknown.[66] Some scholars have noted that despite its decentralised system, the vast majority of Tor's traffic passes through a handful of high bandwidth relays.[67] This suggests that it may be possible to de-anonymise Tor users simply by gaining control of the smaller number of relays that absorb the majority of Tor's traffic.[68]

Moreover, Russia drew media attention in 2014, when it offered a $110,00 reward for anyone who could find a way to de-anonymise Tor users on request.[69] Initially, the company who took on the project achieved poor results, spending more

[62] The Register (`7 July 2020) Seven 'no log' VPN providers accused of leaking – yup, you guessed it – 1.2TB of user logs onto the Internet. Available at: https://www.theregister.com/2020/07/17/ufo_vpn_database/ [accessed 20 September 2020].
[63] Ibid.
[64] Snowden Archive (4 October 2014) TOR stinks. Available at: https://edwardsnowden.com/docs/doc/tor-stinks-presentation.pdf [accessed 1 March 2018].
[65] Ibid.
[66] Ibid.
[67] Levine, Y. *Surveillance valley: the secret military history of the Internet*, [Kindle version] (New York, Public Affairs, 2018), p. 373.
[68] Ibid.
[69] BBC News (28 July 2014) Russia offers $110, 000 to crack Tor anonymous network. Available at: https://www.bbc.co.uk/news/technology-28526021 [accessed 20 June 2017].

than the offered reward to escape what it deemed to be an unachievable contract.[70] Yet, a 2019 hack revealed that the FSB contractor, SyTech, had combined control over a Tor exit-node with so-called 'man-in-the-middle attacks' in an effort to de-anonymise a very select number of Tor users.[71] With man-in-the-middle attacks, Internet users are unwittingly presented with fake copies of the website they originally intended to visit (which can collect personally identifiable information) and by controlling the exit node Russian could, in theory, determine which websites to mimic. Alternatively, SyTech could contrast the times and dates of people using the controlled exit node against Internet Service Provider records, to determine likely culprits. As experts have noted, without wide reaching control over Tor's relays, Russia's success will likely be limited. However, even if Russia and China cannot see what their citizens are doing within a proxy network, they *can* see that someone has connected to those networks.[72] This was illustrated through an NSA programme named XKeyscore (disclosed by Snowden), which harvested the IP addresses of US citizens who connected to Tor or other anonymising tools.[73] It would not be a leap to propose that Russia and China, with their paranoiac surveillance powers, would be inclined to do the same, cataloguing those who connect to proxies.

A recurring problem with these commercial solutions is that they are known to security services, meaning it is easier to scrutinise their traffic, but as claimed in a

[70] Bloomberg (22 September 2015) Russia's plan to crack Tor crumbles. Available at: https://www.bloomberg.com/news/articles/2015-09-22/russia-s-plan-to-crack-tor-crumbles [accessed 1 March 2018]; Meduza (9 September 2015) The Russian government hired people to hack to the Tor browser, but they failed and now they're quitting. Available at: https://meduza.io/en/news/2015/09/09/the-russian-government-hired-people-hack-the-tor-browser-but-they-failed-and-now-they-re-quitting [accessed 1 March 2018].
[71] BBC News (22 July 2019) Russian intelligence 'targets Tor anonymous browser'. Available at: https://www.bbc.co.uk/news/technology-49071225 [accessed 20 September 2020].
[72] Ibid.
[73] Zetter, K. (3 July 2014) The NSA is targeting users of privacy services, leaked codes shows, *Wired*. Available at: https://www.wired.com/2014/07/nsa-targets-users-of-privacy-services/ [accessed 1 March 2018].

series of media reports from 2018, Langley's attempts to design a more secure form of system, with a less overt type of traffic, proved disastrous.[74] As confirmed by multiple official sources, an online covert communications system, first introduced in 2009 and shared with SIS, led to the collapse of operations in various hard target states.[75] Between 2010 – 2012, the CIA lost a swathe of agents in China, Iran, and elsewhere, which officials described as one of the worst intelligence breaches in 'decades'.[76] To explain the losses, Langley initially pointed suspicions toward a former CIA case officer, Jerry Chun Shing Lee, but accusations of his betrayal were tempered by the fact that Lee could not have known all the identities of the sheer number of agents compromised in the breach.[77] Eventually, communications tradecraft fell under the spotlight, and it has since been determined that a compromise of the CIA's online covert communications systems was likely responsible.[78]

According to media reports, the Office of Technical Services designed two systems, one intended for highly valued assets, and the other an interim "throwaway" system for everyone else.[79] Both were 'internet-based and accessible from laptop or desktop computers', and supposedly distinct, meaning if the throwaway system was breached the main system remained safe: '[in] theory, if the interim system were

[74] Huffington Post (12 June 2018) At the CIA, a fix to communications system that left trail of dead agents remains elusive. Available at: https://www.huffingtonpost.com/entry/at-the-cia-a-fix-to-communications-system-that-left-trail-of-dead-agents-remains-elusive_us_5c094117e4b069028dc7696a [accessed 15 March 2019].
[75] Huffington Post (12 June 2018) At the CIA, a fix to communications system that left trail of dead agents remains elusive. Available at: https://www.huffingtonpost.com/entry/at-the-cia-a-fix-to-communications-system-that-left-trail-of-dead-agents-remains-elusive_us_5c094117e4b069028dc7696a [accessed 15 March 2019].
[76] Mazetti, M. et al. (20 May 2017) Killing C.I.A. informants, China crippled U.S. spying operations, *The New York Times.* Available at: https://www.nytimes.com/2017/05/20/world/asia/china-cia-spies-espionage.html [accessed 1 January 2018].
[77] NBC News (20 January 2018) Alleged CIA China turncoat Lee may have compromised U.S. spies in Russia too. Available at: https://www.nbcnews.com/news/china/cia-china-turncoat-lee-may-have-compromised-u-s-spies-n839316 [accessed 1 March 2018].
[78] Ibid.
[79] Dorfman, Z. (15 August 2018) Botched CIA communications system helped blow cover of Chinese agents, *Foreign Policy.* Available at: https://foreignpolicy.com/2018/08/15/botched-cia-communications-system-helped-blow-cover-chinese-agents-intelligence/ [accessed 1 November 2018].

discovered or turned over to Chinese intelligence, people using the main system would still be protected – and there would be no way to trace the communication back to the CIA.'[80] They worked by hiding communications in plain sight, with agents connecting to 'innocuous seeming websites'.[81] But to safely connect to these websites, wherein agents could directly communicate with handlers, they had to perform what officers describe as "electronic surveillance detection routes", meaning to 'bounce around on various sites on the internet before accessing the system, in order to cover their tracks'.[82] Moreover, akin to disguising spy gadgets as everyday items, it seems these tools could be made to appear non-incriminating. During the 2014 arrest of Markus Reichel, a German BND employee who spied for the CIA, investigators discovered a specialised weather app used to message his handlers, one activated by searching for weather forecasts in New York.[83] It is not clear whether Markus used exactly the same system, but it underscores the point that these cyber tools could be easily hidden on the agent's computer as ostensibly ordinary software

Concealing the systems' traffic, however, seems to have proven far more difficult. While originally designed for warzones, the systems soon became a primary means of communication in a broad array of operational theatres, including in countries "with sophisticated counterintelligence operations. Like China".[84] But they were never intended to be a staple of covert communications, nor were they designed to withstand

[80] Ibid.
[81] Huffington Post (12 June 2018) At the CIA, a fix to communications system that left trail of dead agents remains elusive. Available at: https://www.huffingtonpost.com/entry/at-the-cia-a-fix-to-communications-system-that-left-trail-of-dead-agents-remains-elusive_us_5c094117e4b069028dc7696a [accessed 15 March 2019].
[82] Ibid.
[83] Huggler, J. (July 2014) Germany demands full explanation from US on arrested spy, *The Telegraph.* Available at: https://www.telegraph.co.uk/news/worldnews/europe/germany/10949568/Germany-demands-full-explanation-from-US-on-arrested-spy.html [accessed 23 March 2020].
[84] Dorfman, Z. (15 August 2018) Botched CIA communications system helped blow cover of Chinese agents, *Foreign Policy.* Available at: https://foreignpolicy.com/2018/08/15/botched-cia-communications-system-helped-blow-cover-chinese-agents-intelligence/ [accessed 1 November 2018].

scrutiny in places where Internet activity is scrutinised around the clock, or where unusual patterns are flagged. And although the interim system was supposed to be distinct, a technical error meant that the two shared overlapping code, leading one to expose the other, as *Foreign Policy* reported:

> …the CIA's interim system contained a technical error: It connected back architecturally to the CIA's main covert communications platform. When the compromise was suspected, the FBI and NSA both ran "penetration tests" to determine the security of the interim system. They found that cyber experts with access to the interim system could also access the broader cover communications system the agency was using to interact with its vetted sources, according to former officials.[85]

That created a serious vulnerability for the CIA's global assets. As one former official noted, "[all] they had to do was get one agent's laptop, and they could figure it out".[86] According to former intelligence officers, the Iranians were the first to discover how the systems worked, using tactics as simple as Google searches to unravel the network and identify agents, as *Yahoo News* explains:

> … they began to scour the internet for websites with similar digital signifiers or components — eventually hitting on the right string of advanced search terms to locate other secret CIA websites. From there, Iranian intelligence tracked who was visiting these sites, and from where, and began to unravel the wider CIA network.
>
> In fact, the Iranians used Google to identify the website the CIA was using to communicate with agents. Because Google is continuously scraping the internet for information about all the world's websites, it can function as a tremendous investigative tool — even for counter-espionage purposes. And Google's search functions allow users to employ advanced operators — like "AND," "OR," and other, much more sophisticated ones — that weed out and isolate websites and online data with extreme specificity.'[87]

[85] Ibid.
[86] NBC News (20 January 2018) Alleged CIA China turncoat Lee may have compromised U.S. spies in Russia too. Available at: https://www.nbcnews.com/news/china/cia-china-turncoat-lee-may-have-compromised-u-s-spies-n839316 [accessed 1 March 2018].
[87] Yahoo News (2 November 2018) The CIA's communications suffered a catastrophic compromise. It started in Iran. Available at: https://in.news.yahoo.com/cias-communications-suffered-catastrophic-compromise-started-iran-090018710.html?guccounter=1 [accessed 3 November 2018].

Iran was soon suspected of sharing its findings with China, where between 2009-2012 the CIA lost a substantial number of agents. While it remained possible, albeit unusual, that both countries had broken the systems at almost exactly the same time, US intelligence officials were reportedly aware that Iran, Russia, and China were engaging in senior level talks on cyber issues.[88] According to US officials, following a joint training session with China, Russian intelligence officers "came back saying we got good info on covcom", suggesting that efforts against the CIA's systems were global and coordinated.[89] China devoted a joint MSS / PLA task force to the matter, while Iran relentlessly identified agents across the world, forcing the CIA to suspend all cyber communications throughout the entire Middle East.[90] Of the three powers, only in Russia was the damage relatively limited, because intelligence officers quickly adjusted their methods once signs of trouble arose.[91]

Former officials acknowledge that attempts to fix the problem have largely faltered, as one ex-CIA officer noted, it's not just "a single flawed system that needed to be fixed … It was a universe of systems".[92] Officials speaking to the *Huffington Post* expanded on this problem, adding "[a] patch won't solve the problem … We're not talking about billions of dollars, we're talking about hundreds of billions of dollars to fix [these systems]".[93] Although one official claims "there's been major improvement", he hints that current solutions do not appear suitable for hard target conditions: "it

[88] Ibid.
[89] NBC News (20 January 2018) Alleged CIA China turncoat Lee may have compromised U.S. spies in Russia too. Available at: https://www.nbcnews.com/news/china/cia-china-turncoat-lee-may-have-compromised-u-s-spies-n839316 [accessed 1 March 2018].
[90] Yahoo News (2 November 2018) The CIA's communications suffered a catastrophic compromise. It started in Iran. Available at: https://in.news.yahoo.com/cias-communications-suffered-catastrophic-compromise-started-iran-090018710.html?guccounter=1 [accessed 3 November 2018].
[91] Huffington Post (12 June 2018) At the CIA, a fix to communications system that left trail of dead agents remains elusive. Available at: https://www.huffingtonpost.com/entry/at-the-cia-a-fix-to-communications-system-that-left-trail-of-dead-agents-remains-elusive_us_5c094117e4b069028dc7696a [accessed 15 March 2019].
[92] Ibid.
[93] Ibid.

doesn't serve everyone equally".[94] Owing, in part, to what another intelligence officer called "shitty defense contractors", operatives do not expect to have a viable alternative anytime soon.[95] Key to the problem, they argue, is a failure by the CIA's engineers to acknowledge the operational limits of cyberspace "[in] official traffic they say, 'Yes, we can do that.' But over direct message, they'd say, 'We can't'".[96] But a perfect system may not be realistic - by hiding messages in plain sight, the original systems relied on a type of traffic that was relatively innocuous, but they still created signatures that could be identified once counterintelligence knew where to look, meaning in countries where telecommunications and Internet infrastructure is monitored around the clock, this problem cannot be easily resolved.[97]

Combined, these risks place greater weight on the need for trust. At minimum, there are no forms of covert communication tradecraft in the cyber era that are likely an easy sell to serving spies, which means incriminating measures should not be incorporated into the field unless there are assurances that the agent will use them. Personal meetings, dead drops, SRAC, and even upgraded spy rocks, are still highly dangerous and likely uninspiring to those informed of the risks. Even the satellite SIM card smuggled into Cuba raised alarms for Alan Gross, who wrote "we are all 'playing with fire" and that "detection of satellite signals will be catastrophic".[98] Reportedly, Gross only agreed to smuggle the card because he firmly believed that as an American citizen, he would face, at worse, deportation, not a lengthy prison sentence.[99] Cyberspace doesn't seem to offer any greater advantages where trust in technology is

[94] Ibid.
[95] Ibid.
[96] Ibid.
[97] Yahoo News (2 November 2018) The CIA's communications suffered a catastrophic compromise. It started in Iran. Available at: https://in.news.yahoo.com/cias-communications-suffered-catastrophic-compromise-started-iran-090018710.html?guccounter=1 [accessed 3 November 2018].
[98] Bloomberg (12 February 2012) AP impact: USAID contractor work in Cuba detailed. Available at: http://www.businessweek.com/ap/financialnews/D9SSHGPG2.htm [accessed 12 March 2018].
[99] Ibid.

concerned, especially with regards to off-the-shelf systems such as email dead-drops or simple Gmail. But even more advanced systems such as Tor or VPN are increasingly open to doubt. Many citizens could theoretically use these services without recrimination, but in some cases connecting to these services could lead to punishments. In 2015, Uyghur residents from China's Xinjiang province who connected to VPNs suddenly lost access to their mobile services, and were forced to visit local police offices to have their phones restored and, presumably, their data recorded.[100] In fact, China is reportedly losing tolerance for anyone caught using illicit VPN providers, in some cases handing down lengthy prison sentences for those who do so.[101] Similarly, in 2017 Russia arrested Tor relay operator Dmitry Bogatov for accusations of inciting terrorism, after an unknown user co-opted his relay to conduct illegal activities.[102] Most of the charges against the operator were later dropped, but Bogatov's use of the Tor browser was still considered a misdemeanour, and as such some charges were kept, inferring that the Kremlin was keen to make an example of the case.[103] The mere prospect of such punishments could easily deter agents working under Moscow or Beijing conditions, even if they are rare, since although access to a proxy might, in most cases, be treated as a minor misdemeanour, it could also be used as evidence if a person fell afoul of the state, particularly if that person was privy to classified information and suspected of espionage.

[100] Tech Crunch (25 November 2015) China punishes VPN users in its rural northwest by cutting their mobile service. Available at: https://techcrunch.com/2015/11/25/china-punishes-vpn-users-in-its-rural-northwest-by-cutting-their-mobile-service/?_ga=2.42157157.1785373780.1543256229-223957389.1543256229 [accessed 20 June 2017].
[101] Haas, B. (22 December 2017) Man in China sentences to five years' jail for running VPN, *The Guardian.* Available at: https://www.theguardian.com/world/2017/dec/22/man-in-china-sentenced-to-five-years-jail-for-running-vpn [accessed 20 January 2018]; BBC News (11 February 2019) Russia considers 'unplugging' from Internet. Available at: https://www.bbc.co.uk/news/technology-47198426 [accessed 13 February 2019].
[102] Meduza (23 May 2018) Russia finds a new Tor criminal: How Dmitry Bogatov went from suspect to witness. Available at: https://meduza.io/en/feature/2018/05/23/russia-finds-a-new-tor-criminal [accessed 27 May 2018].
[103] Ibid.

Moreover, even if the flaws in the CIA's more advanced cyber systems could be ironed out, many agents, now aware of the dangers through a series of damning headlines, might reasonably reject their use. The severe consequences of the systems' breach, and their widespread public coverage, will inevitably lead to lingering concerns about the long-term reliability of any cyber platform. As one official noted, "[will] a system always stay encrypted, given the advances in technology? You're supposed to protect people forever."[104] Moreover, this is not the first incident to present the CIA's cyber systems in poor terms. In 2004, CIA agents were neutralised throughout Iran after one intelligence officer mistakenly sent an online communication to an Iranian double agent, which contained information about most assets in the region.[105] And while it is impossible to know exactly how present or future agents may feel about the CIA's cyber communications, it would not be illogical to expect a pessimistic answer. This is perhaps best captured by the opinions of intelligence officers, who seem to have almost entirely lost faith in their cyber systems, returning instead to traditional, risky methods such as personal meetings.[106] As one CIA official noted, proponents of old fashioned communications such as brush passes and chalk marks were long considered "troglodytes" by their colleagues, and yet after the devastation caused in Iran and China, the "troglodytes" seem to be leading the way forward.[107] If their handlers don't trust cyberspace, it is hard to see why their agents would.

Furthermore, trust in the agent's competencies and loyalties remains important. Even SRAC, over thirty years after its development, was still reserved only for 'long-

[104] Dorfman, Z. (15 August 2018) Botched CIA communications system helped blow cover of Chinese agents, *Foreign Policy.* Available at: https://foreignpolicy.com/2018/08/15/botched-cia-communications-system-helped-blow-cover-chinese-agents-intelligence/ [accessed 1 November 2018].
[105] James, R. *State of War: the secret history of the CIA and the Bush administration*, [Kindle version] (New York, Simon & Schuster, 2006). Accessed 10 July 2020, see chapter 9.
[106] Yahoo News (2 November 2018) The CIA's communications suffered a catastrophic compromise. It started in Iran. Available at: https://in.news.yahoo.com/cias-communications-suffered-catastrophic-compromise-started-iran-090018710.html?guccounter=1 [accessed 3 November 2018].
[107] Ibid.

established and highly trusted agents.'[108] But this trust dimension was particularly acute for CIA's cyber systems, since all it took was a single laptop to fall into Iranian hands for counterintelligence to develop countermeasures.[109] Langley later tied the breach to an Iranian double agent, who was perfectly positioned to pass said "laptop" to counterintelligence.[110] In addition, while agents were supposed to run "electronic surveillance detection routes" before using the system, many failed to do so, potentially creating suspicious patterns of activity.[111] As a result, one of the largest losses of agents in modern times was caused by a duplicitous asset, and potentially worsened by agents who ignored their training. Assuming, therefore, that the CIA's cyber systems are upgraded, any future iteration would be better reserved only for highly trusted and trained assets. Indeed, considering the fact that a future "fix" is expected to cost billions, if not hundreds of billions, of dollars, it would be a misjudgement to offer these technologies to careless or untrusted spies.

Collection

The fourth and final function of tradecraft is collection, where the agent must safely access and extract their intelligence. Herein, one crucial factor to consider is the digitisation of information, '[while] printed copies still exist within filing cabinets and safes, … documents are also available in IT networks, and it is there that their full utility can be realized'.[112] The storage of secrets within easily accessible networks

[108] Tomlinson, R. *The big breach*, p. 69.
[109] NBC News (20 January 2018) Alleged CIA China turncoat Lee may have compromised U.S. spies in Russia too. Available at: https://www.nbcnews.com/news/china/cia-china-turncoat-lee-may-have-compromised-u-s-spies-n839316 [accessed 1 March 2018].
[110] Ibid.
[111] Huffington Post (12 June 2018) At the CIA, a fix to communications system that left trail of dead agents remains elusive. Available at: https://www.huffingtonpost.com/entry/at-the-cia-a-fix-to-communications-system-that-left-trail-of-dead-agents-remains-elusive_us_5c094117e4b069028dc7696a [accessed 15 March 2019].
[112] Gosler, J. R. 'The digital dimension', in *Transforming U.S. Intelligence, edited by Jennifer E. Sims & Burton Gerber,* (Washington, Georgetown University Press, 2005), p. 100.

means that even low-level sources, with the right permissions, could theoretically access massive volumes of information.[113] Edward Snowden is cited by former SIS officer, Nigel Inkster, as a blatant illustration of this point.[114] Snowden was not an intelligence officer, but a contracted systems administrator responsible for the upkeep and maintenance of NSA systems and networks (and one of around 1000 NSA systems administrators at the time, of a total 40,000 staff).[115] Since it was his job to move classified information across NSA networks (for operations that he was not directly involved in), he was able to access millions of files, despite working from his Hawaiian office five thousand miles from Fort Meade.[116]

Yet in some respects, Snowden's case is less emblematic of the modern agent's outreach, and more indicative of the NSA's failings. According to officials, including NSA Deputy Director Rick Ledgett, who headed the investigation into Snowden's leaks, the Hawaiian branch was one of the last NSA offices to be upgraded with modern security practices.[117] And in the process of his activities, Snowden left ample 'yellow flags', including multiple requests to view Top Secret files without any apparent reason to do so.[118] He even, according to some reports, borrowed (or stole) his colleagues encryption passwords, to access files beyond his own authorisation.[119] In his

[113] Jones, S. (28 September 2016) The spy who liked me: Britain's changing secret service. *Financial Times.* Available at: https://www.ft.com/content/b239dc22-855c-11e6-a29c-6e7d9515ad15 [accessed 1 March 2018].
[114] Ibid.
[115] Business Insider (13 December 2013) NSA: Snowden stole 1.7 million classified documents and still has access to most of them. Available at: http://www.businessinsider.com/how-many-docs-did-snowden-take-2013-12?IR=T [accessed March 1 2018]; NBC News (26 August 2013) How Snowden did it. Available at: http://www.nbcnews.com/news/other/how-snowden-did-it-f8C11003160 [accessed March 1 2018].
[116] Ibid.
[117] Sanger, D. E. & Schmitt, E. (9 February 2014) Snowden used low-cost tool to best N.S.A, *The New York Times.* Available at: https://www.nytimes.com/2014/02/09/us/snowden-used-low-cost-tool-to-best-nsa.html?hp&_r=1 [accessed 23 July 2017].
[118] Computer World (23 March 2017) Snowden's ex-boss offers advice on stopping insider threats. Available at: https://www.computerworld.com/article/3184411/security/snowdens-ex-boss-offers-advice-on-stopping-insider-threats.html [accessed March 1 2018].
[119] One alleged anonymous NSA official told Forbes that Snowden was seen as a 'genius' by the agency, and granted almost full administrative access to NSA's classified programmes. However, even if that

aftermath, officials were able to track Snowden's suspicious patterns of activity within their systems, concluding that he had likely downloaded 1.7 million classified files.[120] But while all the clues necessary to stop his leaks were in place, his office lacked the procedures to spot them in time. This is a common experience, whereby insiders are able to steal copious amounts of information despite leaving a swathe of incriminating access logs for later investigators. As FBI official Eric O'Neill argues, "[it's] much easier getting the secrets out now, but on the flip side, it's also easier for law enforcement and the FBI to track down who had access to the data".[121] A similar experience to Snowden's can be seen with Robert Hanssen, arrested 13 years earlier, who left a wake of digital evidence in federal networks (including searching for his own name in FBI databases for signs of investigations against him), that were later brought to bear in his trial.[122] As with Snowden, the clues were all there, but the FBI failed to seriously spot these signs due to a lack of available resources at the time.[123]

Snowden's leaks thus served as a wake-up call, drawing attention towards more proactive security practices.[124] Senior NSA officials announced sweeping changes, with

---

claim is true, it implies that Snowden's permissions were highly rare, and granted to him specifically because of his allegedly exceptional ability. For more details, see Greenberg, A. (16 December 2013) An NSA co-worker remembers the real Edward Snowden: 'a genius among geniuses', *Forbes*. Available at: https://www.forbes.com/sites/andygreenberg/2013/12/16/an-nsa-coworker-remembers-the-real-edward-snowden-a-genius-among-geniuses/#342cb66e784e [accessed March 1 2018]; Reuters (13 February 2014) NSA memo confirms Snowden scammed passwords from colleagues. Available at: https://www.reuters.com/article/us-usa-security/nsa-memo-confirms-snowden-scammed-passwords-from-colleagues-idUSBREA1C1MR20140213 [accessed March 1 2018]; Computer World (23 March 2017) Snowden's ex-boss offers advice on stopping insider threats. Available at: https://www.computerworld.com/article/3184411/security/snowdens-ex-boss-offers-advice-on-stopping-insider-threats.html [accessed March 1 2018].

[120] Business Insider (13 December 2013) NSA: Snowden stole 1.7 million classified documents and still has access to most of them. Available at: http://www.businessinsider.com/how-many-docs-did-snowden-take-2013-12?IR=T [accessed March 1 2018]

[121] Daily Best (5 May 2017) Is there a Russian mole inside the NSA? The CIA? Both? Available at: https://www.thedailybeast.com/is-there-a-russian-mole-inside-the-nsa-the-cia-or-both [accessed March 1 2018].

[122] Vogel, R. 'Insider threats: The FBI and the Robert Hanssen espionage case, *Journal of the AIPIO (Australian Institute of Professional Intelligence Officers)*, 22:1, 2014, p. 5.

[123] Ibid.

[124] Reuters (13 December 2013) Exclusive: after 'cataclysmic Snowden affair, NSA faces winds of change'. Available at: https://www.reuters.com/article/us-usa-security-nsa/exclusive-after-cataclysmic-snowden-affair-nsa-faces-winds-of-change-idUSBRE9BC0YZ20131213 [accessed 23 June 2017].

measures including 'two-person control of every place where someone could access data and enhancing the security process that people go through and requiring more frequent screenings of systems administrative access'.[125] The latter point on 'frequent screenings of systems administrative access' is particularly important, as the monitoring of what employees – including systems administrators – do within a network is a crucial defence. For instance, as concluded by the FBI in a series of studies, the observation of employee behaviour and the logging of unusual patterns of activity within an organisation, carried dividends in detecting insider threats.[126] And in a post Snowden world, these kind of security measures have become more common, including the tactic of "tagging" documents, triggering 'real-time alarms' whenever someone tries to access them. [127] One such example, revealed by Vault 7, is a digital watermarking tool called 'Scribbles', which the CIA uses to track unauthorised access to documents that are of interest to foreign intelligence actors.[128]

Measures of this nature vastly increase the levels of risks an agent might face when trying to overstep their authorisations. According to the *New York Times*, officials even insist that if Snowden had worked in the NSA's tightly monitored Fort Meade, rather than Hawaii, he 'almost certainly would have been caught'.[129] And while more invasive security practices, such as monitoring employee behaviour, may create complications in liberal democracies, such concerns are unlikely to be shared in

[125] Ibid.
[126] HackersOnBoard (19 November 2013) BlackHat 2013 – Combating the insider threat at the FBI: Real-world lessons learned. Available at: https://www.youtube.com/watch?v=38M8ta13K0Q [accessed 1 March 2018]
[127] Sheffi, Y. *The power of resilience: how the best companies manage the unexpected*, (London, The MIT Press, 2015), p. 234.
[128] Wikileaks – Vault 7: projects. Available at: https://wikileaks.org/vault7/#Scribbles [accessed 20 September 2020].
[129] Sanger, D. E. & Schmitt, E. (9 February 2014) Snowden used low-cost tool to best N.S.A, *The New York Times.* Available at: https://www.nytimes.com/2014/02/09/us/snowden-used-low-cost-tool-to-best-nsa.html?hp&_r=1 [accessed 23 July 2017].

authoritarian regimes.[130] Russia is supposedly so worried about the vulnerability of its most important secrets, that some of its more secure organisations have returned to typewriters and paper documents, curbing any future Snowden of its own.[131]

But access to information is only useful if the agent has a means to copy and extract documents (assuming they cannot be taken home, which would seem to be unlikely where high level secrets are concerned). One enduring option is clandestine photography, which in theory seems more viable in an age where cameras are part and parcel of office culture, '[not] two decades after intelligence services invested tens of millions of dollars to create a small digital camera for spies, camera phones available in every part of the world perform nearly the same functions'.[132] More discrete collection tools, including spy-cameras disguised as pens or watches inbuilt with high quality photographic, video and audio capabilities, are also now widely accessible.[133] But in practice, photography inside a secure institution, whether by smartphone or spy-camera, is still extremely insecure. Although smartphones are common in the average office, they are not necessarily common in high security institutions.[134] This is exemplified by what security specialists call the BYOD problem, meaning 'Bring Your Own Device to Work'.[135] Simply put, allowing personal devices into the workplace often increases employee efficiency, but these items also create complications, including increasing the risk of data leakage.[136] Finding a balance is therefore important in the private sector, yet

[130] Kont, M. et al. 'Insider threat detection study', *NATO Cooperative Cyber Defence Centre of Excellence,* 2018, p. 28-43.
[131] Elder, M. (11 July 2013) Russian guard service reverts to typewriters after NSA leaks, *The Guardian.* Available at: https://www.theguardian.com/world/2013/jul/11/russia-reverts-paper-nsa-leaks [accessed 13 September 2020].
[132] Wallace, R. 'A time for counterespionage', in *Vaults, Mirrors, & Masks: Rediscovering U.S. Counterintelligence,* (Washington, Georgetown University Press, 2008), p. 113.
[133] Brenner, J. *America the vulnerable: inside the new threat matrix of digital espionage, crime, and warfare* (New York, The Penguin Press, 2011), p. 196-197.
[134] Mehan, J. *Insider threat: a guide to understanding, detecting, and defending against the enemy from within,* (Ely, IT Governance Publishing, 2016), p. 231.
[135] Ibid.
[136] Ibid.

secure institutions are more likely to lean on the side of caution; to repeat a previous point, Langley does not allow its employees to bring smartphones into work, and has only recently allowed notes to be taken on laptops rather than paper.[137] Moreover, one new addition to internal security practices is the proliferation of employee screening systems (using X-Ray scanners), adding new complications for the smuggling of prohibited devices into work.[138] Even if an agent can safely smuggle a camera into work, the bigger issue is finding a private space within which to take their shots. By nature of design, spy cameras, hidden in everyday items such as pens or key fobs, still lack view finders, meaning agents would need to hold the device in a particular position to take clear photographs, an act that is increasingly likely to be noticed if they are required to photograph hundreds of documents.[139]

When it comes to information contained in computer systems, agents may be able to forgo photography altogether. Snowden extracted most of his information using a simple USB storage device, an advantage which was, in part, derived from further failings by NSA.[140] As bemoaned by experts, NSA officials "were laying down on the

[137] CIA (18 September 2015) Deputy Director Cohen delivers remarks on CIA of the future at Cornell University. Available at: https://www.cia.gov/news-information/speeches-testimony/2015-speeches-testimony/deputy-director-cohen-delivers-remarks-on-cia-of-the-future-at-cornell-university.html [accessed 1 January 2018].

[138] One company, Scan-X, provides full body scanners to 'airports, courthouses, border crossings, cruise ships, defense, critical infrastructure, government buildings, prisons, law enforcement buildings, ports, public buildings and special event venues'. For more details, see Scan-X Security ltd - Security scanners, X-ray scanners & people screening. Available at: http://www.scanxsecurity.com/people-screening/ [accessed 21 August 2020].

[139] To better explain, a viewfinder is the part of the camera a user looks through to see that the object being viewed is focused. Since a camera disguised as an everyday object would, in order to maintain the illusion, need to lack any visible viewfinder, the object would need to be held at a predetermined position for the agent to know that the camera is focused. That position would then need to be sustained as the agent takes their shots, which after prolonged time may begin to look unnatural. This is exactly the problem that agents faced in the Cold War. Modern technology may lead to more reliable and clearer shots, but it does not change the fact that the agent would need to hover the object above classified documents, in a particular position, for lengthy periods of time, which eventually might arouse suspicions. For more details, see chapter 4.

[140] Computer World (23 March 2017) Snowden's ex-boss offers advice on stopping insider threats. Available at: https://www.computerworld.com/article/3184411/security/snowdens-ex-boss-offers-advice-on-stopping-insider-threats.html [accessed March 1 2018].

job if they didn't disable the USB port".[141] The US Department of Defense completely restricted the use of USB drives on classified networks in 2008, and as of 2015 the ban had still not been lifted, despite 'how impractical it is for them not to be able to transfer files through removable devices'.[142] Even if ports aren't blocked, institutions can monitor who 'attaches a USB device to a computer that has network access or downloads any file'[143] What a person can and cannot connect to a classified network will thus depend on their relative permissions, but if authorisation can be found the agent could maximise their opportunity by delivering malware through the USB.[144] Snowden also used automated software called "web crawlers", which "scraped data" out of the NSA's systems while he worked his day job.[145] Web crawlers are rarely used on the NSA's networks, leaving post-investigators baffled why they went unnoticed.[146] But they underscore the point that the agent can allow software to do the 'collecting' for them, while they focus on other tasks. Indeed, unauthorised disclosures reveal that Langley had developed a catalogue of 'decoy' tools purpose built for agents to innocuously download classified information:

> These attack methods are able to penetrate high security networks that are disconnected from the internet, such as a police record database. In these cases, a CIA officer, agent or allied intelligence officer acting under instructions, physically infiltrates the targeted workplace. The attacker is provided with a USB containing malware developed for the CIA for this purpose, which is inserted into the targeted computer. The attacker then infects and exfiltrates data to removable media. For example, the CIA attack system Fine Dining provides 24 decoy applications for CIA spies to use. To witnesses, the spy appears to be running a program showing videos (e.g VLC), presenting slides (Prezi), playing

[141] Waterman, S. (14 June 2013) NSA leaker Ed Snowden used banned thumb-drive, exceeded access, *The Washington Times.* Available at: https://www.washingtontimes.com/news/2013/jun/14/nsa-leaker-ed-snowden-used-banned-thumb-drive-exce/ [accessed 1 March 2018].
[142] Brenner, J. America the vulnerable, p. 87; Morel, B. *Cyber Insecurity*, [Kindle version] (New York, Page Publishing, 2017), see chapter 6.
[143] Sheffi, Y. *The power of resilience*, p. 234.
[144] Corera, G. *Intercept: the secret history of computers and spies*, [Kindle version] (London, Weidenfeld & Nicolson, 2015). Accessed 10 January 2018, p. 343.
[145] Sanger, D. E. & Schmitt, E. (9 February 2014) Snowden used low-cost tool to best N.S.A, *The New York Times.* Available at: https://www.nytimes.com/2014/02/09/us/snowden-used-low-cost-tool-to-best-nsa.html?hp&_r=1 [accessed 23 July 2017].
[146] Ibid.

> a computer game (Breakout2, 2048) or even running a fake virus scanner (Kaspersky, McAfee, Sophos). But while the decoy application is on the screen, the underlaying system is automatically infected and ransacked.[147]

In some cases, these cyber exploits would collect data and download information directly to the agent's storage device, yet in other cases they could also transmit data back to Langley through the Internet, removing the need for the agent to carry secrets with them.[148] Since every agent's circumstances are different, the Fine Dining toolkits were highly modifiable; intelligence officers were even provided with a broad-ranging survey involving questions about the nature of the targeted system, Internet availability, and whether 'the operator of the tool [will] be watched while the collection is occurring'.[149] The Vault 7 leaks also disclosed a programme known as Brutal Kangaroo, a sophisticated piece of malware designed to breach air-gaps (systems or networks disconnected from the Internet).[150] In practice, the tool is used to attack air-gapped systems without any internal access, by surreptitiously leaping between devices until one is finally connected to the air-gapped system.[151] This has drawn comparison to the 2010 Stuxnet virus, whereby the infection of one laptop eventually spread onto the air-gapped networks of Iran's Natanz nuclear plant, damaging the facility's centrifuges before the virus travelled far beyond its original target.[152] Recent revelations claim that Stuxnet was infected onto Iranian systems by an agent recruited by Dutch intelligence on behalf of the CIA and Mossad, as one official notes, "the Dutch mole was the most

[147] Wikileaks (7 March 2017) Vault 7: CIA hacking tools revealed. Available at: https://wikileaks.org/ciav7p1/? [accessed 21 August 2020].
[148] Ibid.
[149] Wikileaks (7 March 2017) Fine Dining (case officer toolset) concepts. Available at: https://wikileaks.org/ciav7p1/cms/page_20251099.html [accessed 21 August 2020].
[150] Wikileaks – Vault 7: projects. Available at: https://wikileaks.org/vault7/#Scribbles [accessed 20 September 2020].
[151] The Hacker News (22 June 2017) Brutal Kangaroo: CIA-developed malware for hacking air-gapped networks covertly. Available at: https://thehackernews.com/2017/06/wikileaks-Brutal-Kangaroo-airgap-malware.html [accessed August 21].
[152] Quartz (24 June 2017) Wikileaks: the CIA can remotely hack into computers that aren't even connected to the Internet. Available at: https://qz.com/1013361/wikileaks-the-cia-can-remotely-hack-into-computers-that-arent-even-connected-to-the-internet/ [21 August 2020].

important way of getting the virus into Natanz".[153] It is believed that the agent used a USB to infect the devices of systems engineers, who then 'unwittingly' delivered the payload into the centrifugal systems.[154] The point being, malware allows agents to expand their own range - once the virus reaches its intended target, the agent might not even need to retrieve the results, instead malware akin to Brutal Kangaroo can continue leaping until it infects a computer with access to the Internet, delivering its payload of secret information directly to CIA headquarters.[155]

However, as discussed in the previous chapter, Russia and China have taken significant steps to improve their cyber defences, increasing the likelihood that any uploaded malware will be detected. US federal networks, for example, are protected by a system known as EINSTEIN, designed to identify and block malicious intrusions. [156] Systems such as EINSTEIN ensure that when a virus is finally discovered, they can be blocked throughout entire federal networks.[157] In the case of the Office of Personnel Management breach, EINSTEIN initially failed to detect the intrusions, yet the breach was later discovered in a test by a contractor named *CyTech Services.*[158] It underscores the point that although a virus can exist for some time without being noticed, it may, eventually, be uncovered with software patches. That said, sophisticated malware often

[153] Yahoo News (2 September 2019) Revealed: how a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran. Available at: https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAH0unYTO_3FCbroLyqk4XhbV4hBU4AEVLdj8MwLshOYraeKSxB59cqQ6WgHmk7rpBG3jDdbajDmEtwLJirKfyapCsL1pN1-2Yw2RNsn_zXdL9XngDaCj958MNSfHhf4eIAlnx5pgkJgcWjTMjL6SSgbzhurP2W2t-P_17HSClU7C&_guc_consent_skip=1597675156 [accessed 21 August 2020].
[154] Ibid.
[155] The Hacker News (22 June 2017) Brutal Kangaroo: CIA-developed malware for hacking air-gapped networks covertly. Available at: https://thehackernews.com/2017/06/wikileaks-Brutal-Kangaroo-airgap-malware.html [accessed August 21].
[156] Homeland Security – EINSTEIN. Available at: https://www.dhs.gov/einstein [accessed 1 March 2018].
[157] Ibid.
[158] Rohrlick, J. (7 September 2016) How OPM bilked a security contractor that confirmed a major hack, *Foreign Policy.* Available at: http://foreignpolicy.com/2016/09/07/how-opm-bilked-a-security-contractor-that-confirmed-a-major-hack-cytech/ [accessed 1 March 2018].

relies on tools and techniques that are at least partly known to antivirus and firewall vendors, making it easier to detect and investigate breaches.[159] Stuxnet, for instance, was dubbed a 'Frankenstein patchwork of existing tradecraft, code and best practices drawn from the global cyber-crime community'.[160] Similarly, one Vault 7 disclosure, known as UMBRAGE, describes how the CIA borrowed its own capabilities from known Russian toolkits, to cut its operational costs:

> The UMBRAGE team maintains a library of application development techniques borrowed from in-the-wild malware. The goal of this repository is to provide functional code snippets that can be rapidly combined into custom solutions.
>
> Rather than building feature-rich tools, which are often costly and can have significant CI value, this effort focuses on developing smaller and more targeted solutions built to operational specifications.[161]

Alternatively, handlers could give their agents more costly zero day toolkits, which are less likely to be detected, but even these are not guaranteed to remain unnoticed forever. The Vault 7 leaks demonstrate this point, since the disclosures have now given astute counterintelligence actors all the information they needed to upgrade their defences, as former CIA officer Philip Mudd told press, 'this, from the CIA's perspective, is devastating'.[162] Alex McGeorge, a security researcher for cybersecurity firm *Immunity,* notes that the breach has likely set Langley's cyber capabilities back by at least a year, "[all] of these tools and techniques are now burned … The CIA won't want to use them again, and operations using those tools that may be running at this moment will need to have the tools swapped out or abandoned entirely."[163] Other

[159] Farwell, J. P. & Rohozinski, R., 'Stuxnet and the future of cyber war', *Survival,* 53:1, 2011, p. 25
[160] Ibid.
[161] Wikileaks (7 March 2017) Vault 7: CIA hacking tools revealed. Available at: https://wikileaks.org/ciav7p1/cms/page_2621753.html [accessed 1 March 2018].
[162] CNN (8 March 2017) Analyst says Wikileaks dump 'devastating' for CIA. Available at: https://edition.cnn.com/2017/03/08/politics/philip-mudd-cia-wikileaks/index.html [accessed March 1 2018].
[163] Business Insider (8 March 2017) Wikileaks' dump of CIA hacking tools is 'devastating' for the agency – but there may be an upside. Available at: https://www.businessinsider.com/wikileaks-dump-of-cia-hacking-tools-2017-3?r=US&IR=T [accessed 24 August 2020].

security specialists agreed with McGeorge's assessment, with one noting that "[for] incident responders like me, this is a treasure trove".[164]

This problem is particularly acute against sophisticated opponents, such as Russia or China, who might be tempted to use aggressive measures to gain advanced knowledge of these advanced cyber toolkits. This was underscored on 2016, when a criminal hacking group with alleged Kremlin ties, *The Shadow Brokers,* publicly disclosed some of the NSA's most advanced malware tools.[165] The exploits stolen pertained to the agency's Tailored Access Operations group, a division (since absorbed into the NSA's Directorate of Operations) that was, as the *New York Times* describes 'a cyber Skunk Works, akin to the special units that once built stealth aircraft and drones'.[166] The group conducted some of the NSA's most sophisticated and high level hacking penetrations, collecting information deemed so sensitive that it was initially stored within physical safes. The tools used by TAO were customised, built on cutting edge exploits that could penetrate the highest level targets. Precisely how the Shadow Brokers accessed these highly secretive cyber tools has been a point of deep concern for the agency, provoking fears that a 'mole' may have been responsible.[167] Their exposure, akin to the CIA's experience with the Vault 7 leaks, neutered many of the NSA's most highly valued cyber toolkits.[168]

---

[164] Ibid

[165] Yahoo News (13 January 2018) 'Very high level of confidence' Russia used Kaspersky software for devastating NSA leaks. Available at: https://finance.yahoo.com/news/experts-link-nsa-leaks-shadow-brokers-russia-kaspersky-144840962.html?guccounter=2 [accessed March 1 2018].

[166] Shane, S. et al. (12 November 2017) Security breach and spilled secrets have shaken the N.S.A. to its core, *The New York Times.* Available at: https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html [accessed 1 March 2018]; Shane, S. (3 January 2018) Ex-N.S.A. worker accused of stealing trove of secrets offers to plead guilty, *The New York Times.* Available at: https://www.nytimes.com/2018/01/03/us/politics/harold-martin-nsa-guilty-plea-offer.html [accessed 1 March 2018].

[167] Ibid.

[168] Shane, S. et al. (12 November 2017) Security breach and spilled secrets have shaken the N.S.A. to its core, *The New York Times.* Available at: https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html [accessed 1 March 2018].

Once detected, these toolkits will be widely blocked. When Russian antivirus firm Kaspersky Labs upgraded its software to defend against TOA's tools, the NSA allegedly lost access to a considerable flow of intelligence.[169] However, a more concerning threat is that the agent responsible for uploading the malware onto classified systems might then be identified in subsequent investigations. As argued by security specialist Sean Sullivan, in reference to the Vault 7 disclosures, "[the] bigger concern for [CIA], because this involves human intel, is that now that this has been leaked the people who might still have this on their computers will be able to find it, and they might be able to find out who the asset is working for the CIA", adding, "[if] there's only three people who have access to the machine, then that's the bigger concern for the CIA – the safety of the agent or asset."[170] It is not abnormal for security officers to try to determine whether a breach was caused by an insider threat, a point exemplified in the OPM case, where American engineers 'grilled hundreds of employees' to determine if a federal employee had been responsible.[171] That problem, however, may only be magnified if the agent then has to upload another cyber toolkit, in order to replace the one that had been detected and disabled.

Owing to these risks, trust remains a key concern. One immediate problem is whether agents will feel comfortable smuggling cameras, USB thumb drives, or sophisticated malware into high security institutions, again carrying the possibility that incriminating tradecraft could be brought into the field unnecessarily. Agents who are determined to be productive may accept the dangers, but others, especially those who

[169] Ibid.
[170] The Telegraph (20 May 2017) British and US spies at risk after Wikileaks publishes top-secret CIA spyware document. Available at: https://www.telegraph.co.uk/news/2017/05/20/british-us-spies-risk-wikileaks-publishes-top-secret-cia-spyware/ [accessed 1 March 2018].
[171] Koerner, B. I. (23 October 2016) Inside the cyberattack that shocked the US government, *Wired*. Available at: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ [accessed 1 March 2018].

are more concerned with security, have justifiable reason to be perturbed. There is little doubt, for example, that if a person with access to classified information is found to be owning a spy-camera, even a commercial variant, they will face serious consequences. Russia, as a case in point, pressed charges against a farmer who purchased a GPS tracker from China with an inbuilt microphone, because this illicit sensory feature fell under the rules against "special technical equipment for sourcing unofficial information".[172] Then again, others may be determined to take a chance, as underscored by one recently defected CIA asset who allegedly photographed documents sitting on Putin's desk.[173] It isn't clear how he achieved this feat, but if he took the photographs without permission, and especially if he did so in the presence of company, then the agent would have willingly endangered himself.

But USB sticks and cyber tools offer no greater prospects of success. In authoritarian regimes, even the slightest hint of suspicion that a person purposefully infected a classified system may be enough to condemn the source. This was underscored by the Stuxnet case, where, to repeat the point, it seems that Iranian scientists unwittingly uploaded the payload onto the centrifugal systems after their own devices were infected by a Dutch agent.[174] In the aftermath of the incident, Iran arrested several "nuclear spies" purely on suspicion of involvement in the infection, whose fate

[172] RT News (14 December 2017) Cow-nterintelligence: farmer faces 'spy' charges for wiretapping his cow. Available at: https://www.rt.com/news/413152-armer-spy-cow-gps/ [accessed 21 August 2020].
[173] Huffington Post (9 October 2019) CIA reportedly had asset so close to Putin that spy could photograph secret documents. Available at: https://www.huffingtonpost.co.uk/entry/cia-russia-informant-putin-extracted_n_5d76f3b5e4b0fde50c2bbc9b?ri18n=true&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAEL88NGqHuZX2Rf4j8ccflWs0nh5OsAvuEKSmbA1o63umH5m0gjbbZtAcy1D3GlWf6uUXyG8WijoxysZdPU8uBxFt2MPMRvHsEXKYjs-38YREnLmBken4G7MGxBTSjPmTToih8hHmOOV_zUDX4Tia5WTdyg9qin33CPTSujs4cqx&guccounter=2 [accessed 20 September 2020].
[174] Cappelli, D. Moore, A. Trzeciak, R. *The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud)*, (Boston, Addison-Wesley, 2012), p. xxi; Nowroz, M. O. 'Insider threats: detecting and controlling malicious insiders', in *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, edited by Maurice Dawson & Marwan Omar (Hershey, Information Science Reference, 2015), p. 163.

remains unclear.[175] Even the simple act of plugging a USB stick into a classified network without clear authorisation is itself a dangerous one, and unlikely to inspire confidence in concerned agents. Israel's Nuclear Research Center, as a case in point, promptly ended one veteran chemist's career for connecting USB drives fourteen times to classified networks, despite the fact he only did so to upload academic papers.[176] In most cases, it would be far safer for the agent to simply take notes in work, and photograph (or digitally download) any documents that can be taken home, minimising those "yellow flags".[177] As argued by the FBI's former chief Information Technology officer, Patrick Reidy, the spies most likely to succeed in monitored networks will 'laser-focus steal things', rather than create large incriminating signatures.[178] In other words, they will be highly selective in the documents they copy within their working purview, avoiding suspicious patterns of activity.[179] Again, this is highly circumstantial, but it raises the problem that those in the most secure institutions, which contain the most valuable secrets, may be less inclined to use the cyber tools at their disposal.

Trust in the agent's competencies and loyalties also rises in importance, to ensure that agents use collection tools responsibly. Handlers would need to know, for example, that a source would not be careless enough to smuggle a spy camera into an extremely dangerous area, or plug a USB stick into classified networks repeatedly and without permission. They would also, again, need to know that their advanced cyber tools will be safely used, or not gifted straight to counterintelligence by a duplicitous

[175] BBC News (2 October 2010) Iran arrests 'nuclear spies' accused of cyber attacks. Available at: https://www.bbc.co.uk/news/world-middle-east-11459468 [accessed 1 March 2017].
[176] Hovel, R. (16 January 2014) Nuclear researcher fired for connecting USB flash drive to work computer, *Haaretz*. Available at: https://www.haaretz.com/.premium-nuclear-researcher-fired-over-usb-1.5312577 [accessed 1 March 2018].
[177] HackersOnBoard (19 November 2013) BlackHat 2013 – Combating the insider threat at the FBI: Real-world lessons learned. Available at: https://www.youtube.com/watch?v=38M8ta13K0Q [accessed 1 March 2018].
[178] Ibid.
[179] Ibid.

asset.[180] This trust dimension is especially important where highly costly cyber tools are concerned, since not only would their discovery waste an enormous amount of time and resources, but they could also be used to track down other agents who had infected classified networks with the same toolkits.[181] The Vault 7 leaks, for example, had potentially endangered any agent who had used these exposed cyber toolkits at some point in their espionage career.[182] Moreover, the NSA's initial belief that a mole had been responsible for the loss of its TAO cyber weapons, underscores the point that an irresponsible human asset can cause a great deal of damage.[183] In the NSA's case, 'finding, keeping, and safeguarding' its sophisticated cyber exploits is a chief priority, and there is little reason to believe that Langley would feel differently, implying that its most effective exploits – namely those likely to penetrate Russia and China's most secure classified networks – will be reserved for highly trusted assets.[184] Those concerns will have to be balanced against the agent's nature, since there is every risk that if an asset is not given the tools to do the job, they might go out and procure their own clandestine equipment.[185] Since it's a tactic used by leakers such as Snowden and Manning, it would not be a leap to picture an overeager agent purchasing a commercial

[180] It is worth noting that in the Fine Dining survey given to intelligence officers before cyber tools are offered to agents, a distinction is made between 'assets' and 'developmentals'. The latter, in this case, is a person who is still being developed as a trusted asset, implying that levels of trust in the 'operator' had an impact on the kinds of tools at their disposal. For more details, see Wikileaks (7 March 2017) Fine Dining (case officer toolset) concepts. Available at: https://wikileaks.org/ciav7p1/cms/page_20251099.html [accessed 21 August 2020].
[181] The Telegraph (20 May 2017) British and US spies at risk after Wikileaks publishes top-secret CIA spyware document. Available at: https://www.telegraph.co.uk/news/2017/05/20/british-us-spies-risk-wikileaks-publishes-top-secret-cia-spyware/ [accessed 1 March 2018].
[182] Ibid.
[183] Shane, S. (3 January 2018) Ex-N.S.A. worker accused of stealing trove of secrets offers to plead guilty, *The New York Times.* Available at: https://www.nytimes.com/2018/01/03/us/politics/harold-martin-nsa-guilty-plea-offer.html [accessed 1 March 2018].
[184] Loleski, S. 'From cold to cyber warriors: the origins and expansion of NSA's Tailored Access Operations (TAO) to Shadow Brokers', *Intelligence and National Security*, 34:1, 2018, p. 122.
[185] Even spy-cameras can now be purchased on the Internet, at relatively low costs (and ironically, a cursory search of Amazon reveals that most are imported from China). That may be a tempting risk for agent's who are not being given the tools they feel they need by their handlers. For more details, see Brenner, J. America the vulnerable, p. 196-197.

USB stick to download classified files against instruction, or smuggling their smartphone into a classified archive to photograph documents.[186] Those concerns will constantly need to be factored into any decision to give an agent highly risky cyber tools.

Evaluation

This chapter began by assessing the value of online covert communications to handling. While traditional methods, including dead drops, secret writing, burst radio transmissions (including digital spy rocks), and satellite uplinks, remain in use, they are still vulnerable to physical and technical surveillance. But cyberspace has opened up a multitude of pathways, ranging from rudimentary techniques and off-the-shelf anonymisation tools, to in-house covert communication platforms. The chapter has shown that within two Internet surveillance states, concealing both the existence and content of covert communications from counterintelligence is an exceedingly difficult endeavour. This is most apparent where simple techniques are concerned. Although intelligence officers in the past have, as alleged through the Fogle case, at least temporarily relied on basic systems such as Gmail, these are inherently insecure. Owing to the surveillance powers and data localisation laws discussed in the previous chapter, Russian and Chinese security services would face few obstacles in accessing the content and accounts of mainstream email providers.

Alternatively, anonymisation tools such as Virtual Private Networks or The Onion Router can allow agents to mask their Internet activities and access more secure communication systems. By rerouting traffic through relays, these have frustrated

[186] The Guardian (28 November 2010) How 250,000 US embassy cables were leaked. Available at: https://www.theguardian.com/world/2010/nov/28/how-us-embassy-cables-leaked [accessed 16 January 2021].

surveillance around the world, providing a layer of privacy that facilitates a broad range of malicious activity. However, while it is exceedingly difficult for surveillance to see what citizens do within these proxy networks, the security they offer is limited at best. Owing to their popularity, Russia and China have stepped up efforts to de-anonymise proxy users, including using their deep packet inspection technologies and surveillance powers to identify, block, and restrict proxy traffic. In turn, those services that cannot or will not cooperate with the authorities must constantly adapt their systems to stay ahead of national filters. Even in cases where these services remain accessible, they can only conceal what a user does within their networks, but they cannot conceal the fact that a person is connected to these prohibited services.

As revealed through a swathe of unfavourable headlines, the CIA sought to resolve these insecurities by burying agent communications in plain sight. Through an interim system, for lower valued assets, and a main system, for higher value assets, agents were able to covertly message their handlers by visiting seemingly innocuous websites, masking their activities through “electronic surveillance detection routes”. But since the systems were never designed for long term use in hard target conditions, they proved to be extremely insecure. Once their innocuous traffic, which seems to have gone unnoticed for some time, was discovered by counterintelligence, numerous assets were left exposed. Iran successfully detected and identified agents through mere Google searches, before allegedly sharing their techniques with Russia and China. Thus, the CIA’s systems differed from proxy networks in the sense that their traffic was not easily noticed, but in turn, once counterintelligence knew how to identify patterns of activity, they proved just as vulnerable to detection. Whether a system with a more secure form of traffic can be developed remains doubtful, especially for use in states where Internet traffic is monitored around the clock.

These issues lead to greater dependence on the human dimension, not least by decreasing trust in online covert communication systems. Whether due to the extreme and inconsistent punishments handed out by Russian and Chinese authorities to those caught using VPNs or Tor, or due to the series of damning headlines that followed the disclosures of the CIA's cyber systems, a Moscow or Beijing agent is more likely to be sceptical about the benefits of cyber-enabled communication. Some may be willing to take the chance, or welcome alternatives to high risk personal meetings, but others may recognise that their traffic is not guaranteed to stay secure forever. Intelligence officers will also increasingly need to trust that their agents can use these online systems to the safest degree possible. The fact that the interim system was exposed to counterintelligence by an Iranian double agent, and that several assets failed to take necessary security precautions, underscores the importance of reserving their use. If a more secure online covert communication system is developed, it is more likely to be withheld for agents who are thoroughly trusted and tested, ensuring that it does not fall into opposition hands and that its traffic signatures remain unknown.

The problems in handling can, to an extent, be reduced by improving tradecraft in collection. In an age where secrets are increasingly stored inside computer systems, modern agents can vastly expand their access. The highly damaging revelations of Edward Snowden demonstrated this point to global audiences, whereby a single systems administrator managed to steal thousands of classified documents from one of the world's most secure organisations. However, as this chapter has shown, Snowden's Hawaiian office did not follow best practice security measures, and most contemporary agents will risk exposing their espionage by accessing documents outside their working purview. A simple glance at an unauthorised document may leave an incriminating data trail, creating complications for agents who work in heavily monitored networks.

Yet, in the cyber age, the shift from paper to digital documents opens a multitude of doors for collecting secrets. Today's spies can collect masses of documents with simple USB pen drives, or even upload sophisticated malware to collect and transmit secrets on their behalf. Problems arise, however, when classified networks either prohibit storage devices altogether, or are monitored for unauthorised connections. If the agent plugs an electronic storage device into a monitored system without permission, they risk triggering alarms. Moreover, classified networks are highly likely to be protected by advanced cybersecurity systems, meaning if agents upload malware onto secure systems, they cannot rule out the risk of discovery. While it is more cost effective for intelligence officers to supply their agents with patchwork malware, using tools and techniques borrowed from the public domain, these are also more likely to be detected by firewall and antivirus vendors. Alternatively, more expensive 'zero day' capabilities can be built from the ground up, but these still remain vulnerable to discovery by sophisticated opponents. Either way, if malware is detected on a classified network, there is a clear risk that investigations will be undertaken to determine if a spy was responsible for its upload.

These issues further shift the onus onto the human dimension. Agents will again need to trust in technology; some spies may prefer to take the risk and maximise their production, but others, especially those who are more concerned for security, are likely to be off-put by these escalating dangers. On the other hand, intelligence officers will also need to trust that agents will use these tools safely and proportionality. This is especially true in the case of costly cyber tools, since the discovery of malware by counterintelligence could, in theory, lead to the identification of any agents who had used that particular toolkit. An untrustworthy or incompetent agent could, therefore,

cause an extraordinary amount of damage, meaning intelligence officers will need a great deal of confidence in those who use them.

As a consequence, the picture painted here is once again far from optimistic. Although cyberspace clearly creates opportunities for handling and collection, the gains are vastly outweighed by the risks. As with the previous chapter, the reality of cyber-enabled tradecraft in hard target conditions does not seem to mirror the optimistic assumptions observed in the literature review. Throughout both functions of tradecraft, heavy risks increase dependency on trust, either in technology or in the agent, but trust is not easy to develop or maintain in Moscow or Beijing. Thus, it is once again shown that cyberspace leans heavily towards pessimism.

Conclusion
Is your cyber journey really necessary?

Overview: an imperfect solution

This thesis has demonstrated, through an abductive model, and with key conditional assumptions, that in hard target conditions human behaviour is intrinsic to the success or failure of tradecraft, regardless of the degree to which it utilises cyberspace. Tradecraft is often described as an imaginative and adaptive 'art' that can be upgraded, but not replaced, by science. Each new round of innovation opens new doors - as personified by the subminiature spy-cameras that allowed agents to photograph secrets for the first time in high-security institutions – and yet, like any metaphorical masterpiece, human behaviour dictates its outcome. As this thesis has shown, although innovation can open a multitude of doors throughout the various functions of tradecraft, it cannot change the fact that intelligence officers and their methods rely on the behaviour of a third party – the prospective or serving spy. This behavioural factor, which can be difficult to predict and open to doubt, only becomes more important as the risks continue to mount, and yet it cannot be easily addressed. Trust, in people, tradecraft, and technology, permeates espionage, but in the heavily surveilled and vitally important capitals of Moscow and Beijing, trust is at an all-time premium.

I have made it clear that espionage is a distinct form of human intelligence, focused solely on the clandestine recruitment and handling of agents who remain in place, and facilitated by methods collectively dubbed 'tradecraft'. Cyberspace, on the other hand, is a constantly evolving metaphor, the sum of interconnected information technologies and concurrent human interactivity. Espionage's relationship with cyberspace is distinct from more specific practices such as cyber espionage (or hacking), but it remains understudied. Although a small number of scholars perceive

profound, or *optimistic,* implications from cyber-enabled tradecraft, these arguments were shown to be lacking in development or critical analyses, and to not have considered its prospects in hard target conditions. By comparison, those who remain sceptical of cyberspace's impact, the *pessimists,* offer unsubstantiated arguments for their case. To make sense of these disparities, this thesis proposed an abductive model of research, using history to interpret a growing body of cyber evidence. As shown, while contemporary methods are predominantly hidden behind the barriers of official secrecy, there is no shortage of data pursuant to cyberspace itself. Thus, by determining from an appropriately selected historical case study – specifically the Cold War - the factors that matter most to tradecraft's success or failure, the merits of cyber-enabled tradecraft can be weighed. But abduction must be built around conditional assumptions, meaning we must assume from the outset that both intelligence agencies and their opponents will seek to harness and exploit technology.

It is important that this dissertation is situated within the broader context of international relations. It showed that Russia and China have risen to the top of strategic agendas, posing long-term challenges to a US-led international order. Through rising tensions in Eastern Europe and the Pacific, and the exertion of influence through aggressive covert activity, it is clear that the Western world faces a serious strategic revision. But alongside the refocusing of national security strategies, British – US espionage must be front and centre of the intelligence community's response. Spying, despite its mounting difficulties, provides an increasingly vital window into secrets that cannot be gleamed through safer sources of collection, including the masses of intelligence gathered through open sources and technical intelligence. In turn, human sources remain a vital access point to Russia and China's most guarded secrets, most notably intelligence that resides only within the human mind. But converting the

espionage world from decades of counterterrorism, and training a whole new generation of intelligence officers, will not be a simple process. As illustrated by an influx of funding into SIS, and the funnelling of CIA resources towards Russia, espionage agencies face a new agenda, and must reorganise themselves accordingly.

Having established the case for espionage, it is clear that intelligence agencies require real innovation in their tradecraft. This thesis demonstrated that any attempts to revitalise espionage against the two hard target states of Russia and China must account for the spectre of technologically-augmented street surveillance. Street surveillance, meaning the physical observation of intelligence officers, is still etched into Russian and Chinese counterintelligence philosophy. Both states devote enormous resources to this task, and contain those privy to classified information within the panopticons of Moscow or Beijing. By adapting emerging technologies and maximising their access to data, the threat of surveillance is only increasing in intensity. An intelligence officer's cover is laid bare from the moment they pass through an airport, allowing their movements to be monitored with speed and precision. Faced with a rapidly declining ability to meet their quarry, espionage is embracing innovation. Through substantial investment and internal restructurings instigated by senior level officials, the CIA and SIS are re-evaluating their tradecraft, turning towards the opaque benefits of cyberspace as the solution to espionage's hard target problem.

With the hard target problem defined, this dissertation developed a pathway for further research. Building on the already outlined methodological proposals, this section of the dissertation presents the case for a Cold War focused historical analysis, to determine why tradecraft succeeds or fails. It began by establishing the relevance of the case through its parallels to the contemporary surveillance challenge, the optimism of emerging technological solutions, and the availability of data. Key to this case

selection is the fact that US and UK espionage, despite some successes, did not reclaim any serious advantage over the KGB, providing an opportunity to enquire into the causes of failure. The analysis focuses on the four key functions of tradecraft identified in the literature review - recruitment, surveillance, handling and collection. In each stage, it is shown that while twentieth century innovation opened doors, mounting risks led to greater reliance on the behaviour of prospective or serving spies. Intelligence officers needed to trust that their sources and agents would behave in a way that either justified or mitigated risks, but under hard target conditions the development of trust was a near impossibility. Consequently, the outreach of technology and tradecraft was exceptionally low - indeed, the most effective technologies were among the most difficult to bring into the operational theatre. Thus, trust was a necessary condition for tradecraft to succeed, and yet, against panoptic KGB surveillance, its development was a painstaking process, leading to the following hypothesis:

- Justifying and mitigating the risks of tradecraft (and technology) in hard target conditions requires greater trust in the behaviour of the prospective or serving spy. Yet, in such conditions the odds of failure are vastly increased since intelligence officers are less able to meet their sources and agents and have less influence over, and insight into, their behaviour.

This was subsequently tested against the evidence pursuant to the first two functions of tradecraft – recruitment and surveillance. In *recruitment,* it is shown that while the proliferation of social communications and commercial encryption has opened doors for spies to be cultivated and acquired in cyberspace, those prospects are tempered by the consolidation of Russia and China's Internet surveillance infrastructure. Both states have expanded their legal and technical powers, decreasing the likelihood that social or non-covert communications will remain hidden forever. In turn, intelligence officers require confidence in their target's sensibilities, and a common understanding of the need for discretion, a factor which is aided by endemic self-censorship. In *surveillance*,

it is shown that while social media and hacking open pathways to vast amounts of personal information, all of which can aid in recruiting spies, the relative risks continue to mount amongst increasingly robust security practices. In many cases, intelligence officers will depend upon physical access to targeted devices, at the risk of drawing counterintelligence right to the doorstep of their source. To justify these hazards, it is argued that operatives will require confidence that their targets will do or say something of recruitment value. Herein, the issue of self-censorship is reversed, because those in sensitive positions are least likely to behave indiscreetly, out of fear of surveillance by their own security services.

This is followed by the second two functions of tradecraft - handling and collection. This dissertation demonstrated that online covert communications can open doors for agent *handling*, but the ability to conceal information through heavily surveilled Internet infrastructure is rapidly dwindling. It shows that while commercial systems such as VPNs and Tor have become prominent targets of government surveillance, intelligence agencies can create, and have created, their own systems to circumvent such scrutiny. However the problem of creating innocuous signals in an insecure Internet continues to mount, and as such it is shown that trust is yet again an increasingly important factor. Through the publicization of the CIA's disastrous online communication systems, agents are unlikely to trust in the security that cyberspace might afford.[1] And even if they are willing to take the chance, handlers must have a high degree of confidence that their agents will safely protect expensive and highly vulnerable capabilities. In *collection*, it is argued that through the digitisation of secrets, today's agents can smuggle their data through microelectronic devices or by uploading

[1] Dorfman, Z. (15 August 2018) Botched CIA communications system helped blow cover of Chinese agents, *Foreign Policy.* Available at: https://foreignpolicy.com/2018/08/15/botched-cia-communications-system-helped-blow-cover-chinese-agents-intelligence/ [accessed 1 November 2018].

malware to automate the collection on their behalf. Here, it is shown that the tightening of internal security measures increases the risks of the agent's discovery and limits the utility of technical collection tradecraft. Some agents are likely to reject the use of technology in the workplace out of fear of incrimination, while intelligence officers will yet again require confidence that their assets will use any resources safely. This is particularly apt for malware, since despite their benefits, the cyber tools most likely to breach Russia and China's most guarded systems are also most likely to carry heavy losses if discovered.

What this thesis has therefore shown, is that cyberspace does not provide espionage the advantage it requires to pierce these hard target states. In fact, the opposite is true - espionage is heavily disadvantaged in the cyber era. In order to provide intelligence officers the 'advantage', cyberspace would need to reduce their dependency on increasingly dangerous personal meetings, to a point that allowed high level Russian and Chinese officials to be safely recruited and handled. The majority of intelligence can be gathered through safer means of collection, such as TECHINT or OSINT, which means that the people espionage most needs to recruit are also those with access to heavily protected secrets. But while this thesis has demonstrated that cyberspace can, and will, open doors in very select conditions, when pitted against aggressive and heavily resourced counterintelligence, those conditions are severely constrictive. As the risks mount, human behaviour begins to play an increasingly important role, and yet, since tradecraft is supposed to *reduce* dependency on personal meetings, intelligence officers essentially face a paradox. They need to trust that their agents can and will behave in a manner that is required for tradecraft to succeed, but they cannot build that trust without having secure tradecraft at their disposal. This barrier afflicts every function of tradecraft, and unless there are radical changes to

cyberspace as a whole, it is unlikely to be resolved. Thus, when it comes to recruiting and handling spies in Moscow or Beijing, where the bulk of targets reside, cyberspace is not the 'golden opportunity' that intelligence agencies require.

Implications: one step forwards, two steps back

Given the limitations of abduction, it is impossible to determine the exact scenarios that will arise as a result of cyberspace. It cannot be said for certain, for example, which agents will be recruited, what intelligence will be found, and what political events will unfold. It is perfectly possible that an agent at least partially recruited or handled through cyberspace may help to avoid the next Cuban Missile Crisis or a conflict in the South China Sea, but it is beyond the scope of abduction to make that prediction. However this dissertation has shown that espionage's relationship with technology can be broadly understood through the confines of abductive reasoning. Although abductive predictions within quasi-open social systems are constrained to 'crude qualitative assessments', this is nevertheless sufficient to determining the *probabilistic* outcomes of cyber-enabled tradecraft.

This dissertation's predictions are, however, dependent on two key conditional assumptions. First, it is assumed that intelligence officers, akin to their predecessors, will not ignore the advantages that technology affords. In the Cold War, demand for espionage led intelligence agencies to invest inordinate resources in tools, technologies, and training which were only applied to a very select number of cases. But despite their high costs, the mere possibility of recruiting and handling a source such as Tolkachev in an environment such as Moscow, was seen to be well worth the return on investment. It is indicative that despite the fact that only a small number of agents benefitted from gadgets such as Discus or Tropel, the CIA was prepared to invest millions of dollars in

the Office of Technical Services. It would thus be fair to assume that despite the limitations of cyber-enabled tradecraft, intelligence agencies will still want to invest in the skills and resources required to harness its advantages. Simply put, given the importance of espionage against hard target states, they will likely want to ensure that they have the resources and outreach required to seize an opportunity, rather than miss a chance to recruit or handle an invaluable agent. This, as has been shown, is supported by the efforts of intelligence agencies to develop cutting edge capabilities, as echoed by the advanced CIA cyber tools disclosed by Wikileaks.[2] And while spending on technology is constrained by budgetary limitations, there are few indications that this propensity for innovation will discontinue in the years to come.

The second assumption is that Russian and Chinese counterintelligence will take actions to negate the prospects of cyber-enabled tradecraft to their opponents. Given, however, that both states are concerned by the threat of foreign espionage, and have maintained a legacy of near paranoic security, it seems fair to presume that they will recognise the potential dangers that cyberspace poses. Both states continue to be classed as 'hard targets', and each have proven highly capable when it comes to offensive and defensive cyber practices. This dissertation has shown, through gradually emerging evidence, that both states have sought to mitigate their opponents cyber-enabled practices, often through draconian measures. The very fact that a Chinese MSS / PLA taskforce was able to unravel the CIA's premier covert communications systems, with the aid of Iranian intelligence, is indicative of their determination to address any perceivable threats.[3] Cracks in their defences can, and may occur, as underscored by

[2] Wikileaks (7 March 2017) Vault 7: CIA Hacking Tools revealed. Available at: https://wikileaks.org/ciav7p1/ [accessed 23 December 2020];
[3] Yahoo News (2 November 2018) The CIA's communications suffered a catastrophic compromise. It started in Iran. Available at: https://in.news.yahoo.com/cias-communications-suffered-catastrophic-compromise-started-iran-090018710.html?guccounter=1 [accessed 3 November 2018].

Russia's apparent susceptibility to foreign hacking, creating opportunities that savvy opponents can exploit, but unless extreme change occurs, such as a complete divergence in political and institutional philosophy, their status as hard targets seems likely to endure. If these conditions remain consistent, the implications for espionage offers little room for optimism, since as both sides strive for an advantage over the other, the outcome clearly favours the hard targets.

Clear complications emerge throughout the recruitment and surveillance stage, since in hard target conditions building any form of interpersonal relationship with a person who is not aware of the need for discretion, is becoming more difficult. Given the inherent risks tied with cyber-enabled tradecraft in the recruitment and surveillance functions, and the absence of means to develop trust in the target's behaviour, it is thus hard to see how today's spies can be safely cultivated in modern Moscow or Beijing. Online volunteering would eliminate the need for a drawn out cultivation process, but this rests on the possibilities of a secure approach. It would not be difficult to imagine, for example, a disgruntled official sending a message to the CIA's website from an Internet café, including a temporary email address as a means of response. But intelligence officers in hard targets cannot overlook the threat of a counterintelligence provocation, meaning this tactic would depend upon volunteers being prepared to provide incriminating bona fides through tentatively secure means. That risks reducing espionage's outreach to a handful of sources who understand the means of securing a response, and who are willing to take the gamble. The core problem for handling and collection is the length of time required before agents can be granted access to more secure, or efficient, forms of cyber-enabled tradecraft. As has been shown, multi-billion dollar online covert communication systems and advanced cyber toolkits are clearly at handlers disposal, but these are not the type of tools that can be supplied to untrained

and untested assets. The issue, therefore, is how agents can be sustained in hard target conditions without recourse to reliable tradecraft. Only when sufficiently trusted, are agents likely to be supplied with cyber-enabled solutions, but this doesn't resolve the problem of safely navigating assets to this stage.

It thus seems far more likely that the outreach of espionage inside Moscow or Beijing is extremely limited. Instead, operatives may be better served following in the footsteps of their Cold War predecessors, pursuing the handful of targets who have at least some degree of leeway to travel abroad. The prospects of cyberspace are multiplied if there is freedom to develop trust between the parties, therefore the opportunities that a friendly environment provides for face-to-face encounters cannot be undervalued. In London, an SIS recruiter could develop bonds with a Chinese diplomat to the point where they feel secure in asking for social communications to be constrained to encrypted platforms. Similarly, having learned that the target has a habit of venting their frustrations while intoxicated, the operative may feel emboldened to surreptitiously enter the target's apartment and infect their devices with eavesdropping malware. Alternatively, a CIA handler based in Istanbul could potentially spend weeks, months, or even years training and preparing their agent for a return to Moscow. By which point, the agent could enter hard target conditions with the cyber tools at their disposal to maintain communications or gather valuable intelligence. But there are no easy answers even in this respect, given that a trained and trusted asset may still remain unconvinced of technology's benefits. And, in the absence of perfect solutions, it might otherwise be simpler to adopt SIS's approach with Oleg Gordievsky, keeping agents "on ice" whenever they return home to Moscow or Beijing.

Closing thoughts

The findings of this thesis are significant on two counts. First, there is the dire implication that espionage is not well positioned to meet policymakers' needs. Although cyberspace will, in some situations, give intelligence officers an advantage they otherwise would not have, it is unlikely to offer the complete window into Russian and Chinese affairs that policymakers ultimately desire. This should not be mistaken as a further argument for the declining relevance of HUMINT – espionage is more important than it has been for decades, and will require substantial funding to ensure that necessary opportunities can be seized. Rather, it shows that the intelligence community as a whole faces substantial challenges in meeting policymakers requirements; there are no simple replacements for espionage, which places greater onus on its limitations. In turn, states must accept that events can occur that intelligence officers cannot foresee, not because of a failure of organisation or planning, but because espionage in today's world remains disadvantaged.

This thesis has also resolved the literature's disparity between the optimists and pessimists, at least in specific conditions. It is quite clear that the sceptics, who remained doubtful of the opportunities of modern technology, are ultimately correct - at least where hard target conditions are concerned. However, it must be noted that while the optimists made flawed assumptions about cyber-enabled tradecraft, these arguments were generally broad and not specifically focused on cyberspace's use in Russia and China. In that sense, the optimists were, in a way, also correct. Cyberspace does carry profound value to espionage, but only when the opposing side is more constrained by concerns of legality, civil liberty, and proportionality. It is Russia and China's willingness to cultivate fear, erode online freedoms, and implement draconian measures, that has essentially curtailed cyberspace's benefits. But in a state such as the

UK, the advantage could be reversed. Indeed, the fact that China has recruited and cultivated thousands of sources through LinkedIn, only underscores the point that cyberspace empowers the West's opponents.[4] This thesis has also shown that through abduction, cyber enabled tradecraft can be assessed, meaning there is ample opportunity for more rigorous scholarship. Furthermore, the literature can be enriched by taking into account not just the merits of technology, but the crucial dimension of human behaviour, a lesson that is hard to ignore when the modern world is viewed through the prism of history. In that sense, this thesis offers the foundations for further research, and can guide future investigations both of tradecraft's past, and of the impact of technology in the decades to come.

Furthermore, while it is currently weighted towards pessimism, it is possible that radical technological change could alter such an outlook. Future scholars may wish to consider the potential impact of hypothetical developments, including the encryption of metadata and quantum computing. The encryption of metadata could restrict governments' ability to monitor the what, where, and when of data, meaning activity in cyberspace could become harder to monitor, and communications, as well information, could be shared more freely.[5] This would, in theory, dramatically impact Internet surveillance, and allow communications to be sent more securely through both recruitment and handling. Similarly, quantum computing could render today's encryption standards extremely vulnerable, providing enormous advantages to the use of malware through surveillance and collection.[6] Although some progress has been

[4] Cuthbertson, A. (11 December 2017) China is spying on the west using LinkedIn, intelligence agency claims, *Newsweek.* Available at: http://www.newsweek.com/china-spying-west-using-linkedin-743788 [accessed 1 January 2018].
[5] MIT News (26 February 2020) Protecting sensitive metadata so it can't be used for surveillance. Available at: https://news.mit.edu/2020/protecting-sensitive-metadata-from-surveillance-0226 [accessed 15 January 2021].
[6] MIT Technology Review (30 May 2019) How a quantum computer could break 2048-bit RSA encryption in 8 hours. Available at: https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/ [accessed 15 January 2020].

made in both cases, they also remain very much in their infancy, yet both raise serious questions as to the future of cyberspace. That said, scholars would be unwise to assume that any innovation will not be met by a counterintelligence response, since as yet, there has been no technological advantage that hard targets have not undermined in some way. Regardless of what doors the future opens, mounting risks will inevitably push up the importance of trust in the prospective or serving spy. And - assuming that espionage agencies and their counterintelligence opponents harness technology's opportunities - people, along with their fears, vulnerabilities, and unpredictable characteristics, will ultimately remain the deciding factor for tradecraft's success or failure. This was true in the Cold War, and it is just as true for the cyber age. In fact, if there is to be one underlying takeaway from this thesis and its multiple historical parallels, it is that the more espionage seems to change, the more it also seems to stay the same.

Bibliography

Books and book chapters

Absher, K. M, Desch, M. C., & Popadiuk, R. *Privileged and confidential: the secret history of the president's intelligence advisory board* (Lexington, University Press of Kentucky, 2012).

Aldrich, R. J. *GCHQ: the uncensored story of Britain's most secret intelligence agency* [Kindle version] (London, HarperPress, 2010).

Althoff, M. 'Human intelligence', in *The five disciplines of intelligence collection*, edited by Mark M. Lowenthal &Robert M. Clark (Thousand Oaks, CQ Press, 2016).

Andrew, C. & Mitrokhin, V. *The Mitrokhin archive: the KGB in Europe and the West* (London, Penguin Books, 2000).

Andrew, C. 'Remembering the Cuban missile crisis: memoirs, oral history and lieux de mémoire' in An International History of the Cuban Missile Crisis: A 50-Year Introspective, edited by David Gioe, Len Scott and Christopher Andrew (London, Routledge, 2014).

Andrew, C. Defence of the realm, [Kindle version] (London, Penguin Books, 2010).

Andrew, C. *For the President's eyes only: secret intelligence and the American presidency from Washington to Bush*, (New York, HarperPerennial, 1996).

Applegate, S. 'Cyber conflict: disruption and exploitation in the digital age' in *Current and emerging trends in cyber operations: policy, strategy and practice*, edited by Frederic Lemiuex, (London, Palgrave Macmillan, 2015).

Asplen, C. 'DNA databases', *in Forensic DNA Applications: an Interdisciplinary Perspective*, edited by Dragan Primorac and Moses Schanfield (Boca Raton, CRC Press, 2014).

Bagley, T. H. *Spy wars: moles, mysteries, and deadly games*. [Kindle version] (New Haven, Yale University Press, 2007).

Bamford, J. *The shadow factory: the Ultra-Secret NSA from 9/11 to the eavesdropping on America* [Kindle version] (New York, DoubleDay, 2008).

Barron, J. *KGB: the secret work of Soviet secret agents* (New York, Bantam Books, 1974).

Bartlett, J. *The dark net: inside the digital underworld*, (London, William Heinemann, 2014).

Berkeley, R. *A spy's London*, (Barnsley, Pen & Sword Military, 1994).

Berkowitz, B. *The new face of war: how war will be fought in the 21st century* (New York, The Free Press, 2003).

Betz, J. D. & Stevens, T. *Cyberspace and the state: toward a strategy for cyber power* [Kindle version] (Abingdon, Routledge 2011).

Blaikie, N. *Designing social research: the logic of anticipation* (Cambridge, Polity Press, 2010).

Brenner, J. *America the vulnerable: inside the new threat matrix of digital espionage, crime, and warfare* (New York, The Penguin Press, 2011).

Brope, R. 'Russia', in *Routledge Companion to Intelligence Studies*, edited by Robert Dover, Michael S. Goodman, and Claudia Hillebrand, (Abingdon, Routledge, 2013).

Brown, N. 'The path towards NEC: France, Germany and the United Kingdom', in *Technological Innovation and Defence: The Forza NEC Program in the Euro-Atlantic Framework*, edited by Alessandro Marrone, Michele Nones and Alessandro R. Ungaro (Roma, Edizioni Nuova Cultura, 2016).

Buchanan, B. *The cybersecurity dilemma: hacking, trust, and fear between nations* (Oxford, Oxford University Press, 2016).

Cappelli, D. Moore, A. Trzeciak, R. *The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud),* (Boston, Addison-Wesley, 2012).

Che, X. & Ip, B. *Social networks in China*, (Cambridge, Massachusetts, Chandos Publishing, 2018).

Cialdini, R. B. & Guadagno, R. E. 'Online persuasion and compliance: social influence on the Internet and beyond, in *The Social Net: The Social Psychology of the Internet*, edited by Y. Amichai-Hamburger, (Oxford, Oxford University Press, 2009).

Clark, R. *Intelligence collection,* (Thousand Oaks, CQ Press, 2014).

Clarke, R. A. & Knake, R. K. *Cyber war: the next threat to national security and what to do about it,* [Kindle version] (New York, HarperCollins, 2010).

Copeland, M. *The real spy world* (London, Weidenfeld & Nicolson, 1975).

Cordesman, J. G. *Cyber-threats, information warfare, and critical infrastructure protection: defending the U.S. homeland,* (Westport, Praeger, 2002).

Corera, G. *Intercept: the secret history of computers and spies,* [Kindle version] (London, Weidenfeld & Nicolson, 2015).

Corera, G. *The art of betrayal: life and death in the British secret service,* [Kindle version] (London, Weidenfeld & Nicolson, 2011).

Davies, P. H. J. *MI6 and the machinery of spying,* (London, Frank Cass, 2004).

Deibert, R. & Rohozinski, R. 'Beyond denial: introducing next-generation information access controls', in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace,* [Kindle version] (London, The MIT Press, 2010).

Deibert, R. & Rohozinski, R. 'Control and subversion in Russian cyberspace', in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace,* [Kindle version] (London, the MIT Press, 2010).

Deibert, R. J. *Black code: inside the battle for cyberspace,* (Toronto, McClellend & Stewart, 2013).

Dulles, A. W. *The craft of intelligence: America's legendary spy master on the fundamentals of intelligence gathering for a free world,* (New York, The Lyons Press, 2006).

Duvenage, P. & Von Solms, S. 'Putting counterintelligence in cyber counterintelligence: back to the future', *Proceedings of the 13th European Conference on Cyber Warfare and Security*, edited by Andrew Liaropoulos and George Tsihrintzis, (Reading, Academic Conferences and Publishing International Limited, 2014).

Duvenage, P., Von Solms, S. & Corregedor, M. 'The cyber counterintelligence process – a conceptual overview and theoretical proposition', *Proceedings of the 14th European Conference on Cyber Warfare & Security*, edited by Nasser Abouzakhar, (Reading, Academic Conferences and Publishing International Limited, 2014).

Edgard, T. H. *Beyond Snowden: privacy, mass surveillance, and the struggle to reform the NSA,* (La Vergne, Brookings Institution Press, 2017).

Eftimiades, N. 'China', in *Routledge Companion to Intelligence Studies*, edited by Rovert Dover, Michael S. Goodman, and Claudia Hillebrand (London, Routledge, 2014)

Eftimiades, N. *Chinese Intelligence Operations,* [Kindle version] (Ilford, Frank Cass, 1994).

Ekman, A. 'China's adaptive Internet management strategy after the emergence of social networks', in *Chinese Cybersecurity and Defense,* edited by Daniel Ventre (London, ISTE, 2014).

Enerstvedt, O. M., *Aviation security, privacy, data protection and other human rights: technologies and legal principles,* (Cham, Springer international publishing, 2017).

Feldbrugge, F. J. M. *Russian law: the end of the Soviet system and the role of law,* (Dordrecht, Martinus Nijhoff Publishers, 1993).

Ferris, J. 'Netcentric warfare, C4ISR and information operations: towards a revolution in military intelligence?', in *Understanding Intelligence in the Twenty-First Century, edited by L. V. Scott and P. D. Jacking',* (London, Routledge, 2004).

Fischer, B. B. 'Deaf, dumb, and blind: the CIA and East Germany', in *East German Foreign Intelligence: Myth, Reality and Controversy*, edited by Kristie Macrakis, Helmut Muller-Enbergs, and Thomas Wegener Friis, (Abingdon, Routledge, 2010).

Fouberg, E. H. & Murphy, A. B. *Human geography: people, place, and culture*, (Hoboken, Wiley, 2015).

Gaines, L. K. & Miller, R. L. *Criminal justice in action: 10th edition,* (Boston, CENGAGE, 2019).

Gates, K. A. *Our biometric future: facial recognition technology and the culture of surveillance,* (New York, New York University Press, 2011).

Gill, P. & Phythian, M. *Intelligence in an insecure world,* (Cambridge, Polity Press 2006).

Gill, P. 'Theories of intelligence', in *The Oxford Handbook of National Security Intelligence, edited by Loch K. Johnson,* (Oxford, Oxford University Press, 2010).

Gioe, D. 'Handling HERO: joint Anglo-American tradecraft in the case of Oleg Penkovsky', in *An International History of the Cuban Missile Crisis,* edited by David Gioe, Len Scott, & Christopher Andrew, (London, Routledge, 2014).

Gioe, D. V. 'The more things change': HUMINT in the cyber age', in *The Palgrave Handbook of Security, Risk and Intelligence,* edited by Robert Dover, Huw Dylan, and Michael Goodman (London, Palgrave, Macmillan, 2017).

Gosler, J. R. 'The digital dimension', in *Transforming U.S. Intelligence, edited by Jennifer E. Sims & Burton Gerber,* (Washington, Georgetown University Press, 2005).

Greenwald, G. *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state,* (New York, Metropolitan Books, 2014).

Grey, S. *The new spymasters: inside espionage from the Cold War to global terror,* (New York, Viking, 2015).

Grimes, S & Vertefeuille, J. *Circle of treason: a CIA account of traitor Aldrich Ames and the men he betrayed,* [Kindle version] (Annapolis, Naval Institute Press, 2012).

Guo, X. *China's security state: philosophy, evolution, and politics*, (New York, Cambridge University press, 2012).

Hannas, W. C, Mulvenon, J. & Puglisi, A. B. *Chinese industrial espionage: technology acquisition and military modernization*, (London, Routledge, 2013).

Haseltine, E. *The spy in Moscow station: a counterspy's hunt for a deadly Cold War threat,* [Kindle version] (New York, Thomas Dunne Books, 2019).

Herman, M. *Intelligence power in peace and war,* (Cambridge, Cambridge University Press, 1996).

Hitz, F. P. *The great game: the myths and reality of espionage,* [Kindle version] (New York, Vintage, 2005).

Hitz, F. P. *Why spy? Espionage in an age of uncertainty,* [Kindle version] (New York, St. Martin's Press, 2011).

Hutchings, R. *Soviet secrecy and non-secrecy,* (London, MacMillan Press, 1987).

Imam, J., Reyaz, R., Rana, A. K. & Yadav, V. K. 'DNA fingerprinting: discovery, advancements, and milestones', in *DNA Fingerprinting: Advancements and Future Endeavours,* edited by Hirak Ranjan Dash, Pankaj Shrivastava, Braja Kishore Mohapatra, and Surajit Das (Singapore, Springer, 2018).

Inkster, N. 'The Chinese intelligence agencies: evolution and empowerment in cyberspace', in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, & Reveron, D. S. (Oxford, Oxford University Press, 2015).

Inkster, N. *China's Cyber Power*, [Kindle Version] (Abingdon, Routledge, 2016).

Jackson, P. T. *The conduct of inquiry in international relations: philosophy of science and its implications for the study of world politics,* (London, Routledge, 2011).

James, R. *State of War: the secret history of the CIA and the Bush administration*, [Kindle version] (New York, Simon & Schuster, 2006).

Jeffrey, K. *MI6: the history of the Secret Intelligence Service 1909-1949* (London, Bloomsbury, 2011).

Jervis, R. *Why intelligence fails: lessons from the Iranian Revolution and the Iraq War,* (Ithaca, Cornell University Press, 2010).

Johnson, L. K. *National security intelligence: secret operations in defense of the democracies,* (Cambridge, Polity, 2012).

Johnson, W. R. *Thwarting enemies at home and abroad: how to be a counterintelligence officer* (Washington, Georgetown University Press, 2009).

Jones, H. S. & Towse, J. 'Examinations of email fraud susceptibility: perspectives from academic research and industry practice', in *Psychological and Behavioral Examinations in Cyber Security,* (Hershey, IGI Global, 2018).

Kahn, D. *The codebreakers: the story of secret writing,* (New York, Scribner, 1996).

Kennedy, R. *Of knowledge and power: the complexities of national intelligence,* (Westport, Praeger Security International, 2008).

Kizza, J. M. *Guide to computer network security: fourth edition,* (New York, Springer, 2017).

Klimburg, A. *The darkening web: the war for cyberspace*, [Kindle version] (New York, Penguin Books 2018).

Langlo, H-I. 'Competing academic approaches to cyber security', in *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*, edited by Karsten Friis and Jens Ringmose, (London, Routledge, 2016).

Latell, B. *Castro's secrets: the CIA and Cuba's intelligence machine*, (New York, Palgrave, 2012).

Lawson, J. M. *Critical realism and housing research,* (London Routledge, 2006).

Levine, Y. *Surveillance valley: the secret military history of the Internet*, [Kindle version] (New York, Public Affairs, 2018).

Libicki, M. C. *Conquest in cyberspace: national security and information warfare,* (Cambridge, Cambridge University Press, 2010).

Lowenthal, M. *Intelligence: From secrets to policy*, [Kindle version], (Thousand Oaks, CQ Press, 2017).

Lucas, E. *Cyberphobia: Identity, Trust, Security and the Internet,* [Kindle version] (New York, Bloomsbury, 2016).

Lucas, E. *Deception: Spies, lies, and how Russia dupes the West,* (London, Bloomsbury Publishing PLC, 2013).

Lucas, E. *Spycraft rebooted: how technology is changing espionage*, [Kindle version], (Seattle, Amazon Publishing, 2018).

Macrakis, K. *Seduced by secrets: inside the Stasi's spy-tech world,* [Kindle version] (Cambridge, Cambridge University Press, 2008).

Macrakis, *Prisoners, lovers, & spies: the story of invisible ink from Herodotus to al-Qaeda,* (New Haven, Yale University Press, 2014).

Maddrell, P. *Spying on science: Western intelligence in divided Germany 1945-1961,* (Oxford, Oxford University Press, 2006).

Mahmood, S. 'Online social networks and terrorism: threats and defenses', in *Security and Privacy Preserving in Social Networks*, edited by Richard Chbeir & Bechara Al Bouna (London, Springer, 2013).

Mankoff, J. *Russian foreign policy: the return of great power politics*, (Lanham, MD, Rowman & Littlefield Publishers, 2012).

Marchetti, V. & Marks, J. D. *The CIA and the cult of intelligence,* (London, Jonathan Cape, 1974).

Matthews, M. *Party, state, and citizen in the Soviet Union: a collection of documents,* (London, M. E. Sharpe, 1989).

McCauley, M. *The Cold War 1949-2016*, (London, Routledge, 2017).

Mehan, J. *Insider threat: a guide to understanding, detecting, and defending against the enemy from within,* (Ely, IT Governance Publishing, 2016).

Mendez, A., Mendez J., & Baglio, M. *The Moscow rules: the secret CIA tactics that helped America win the Cold War,* (New York, Public Affairs, 2019).

Mitnick, K. D. & Vamosi, R. *The art of invisibility: the world's most famous hacker teaches you how to be safe in the age of big brother and big data* [Kindle version] (New York, Hachette Book Group, 2017).

Mitrokhin, V. *KGB lexicon: The Soviet intelligence officer's handbook,* (London, Frank Cass, 2002).

Monaghan, A. *The new politics of Russia: interpreting change,* [Open Access e-book] (Manchester, Manchester University Press, 2016).

Morel, B. *Cyber Insecurity,* [Kindle version] (New York, Page Publishing, 2017).

Morgus, R. 'The spread of Russia's digital authoritarianism', in *Artificial Intelligence, China, Russia and the global order,* edited by Nicholas D. Wright, [Kindle version] (Maxwell, Air University Press, 2019).

Nalbandov, R. *Not by bread alone: Russian foreign policy under Putin,* (Lincoln, Nebraska, Potomac Books, 2015).

Nardi, B. *My life as a Night Elf Priest: An Anthropological Account of World of Warcraft,* (Ann Arbor, The University of Michigan Press, 2010).

Nitsch, H. & Irani, D. 'Prevention, anti-radicalisation and the role of social media: a view from Germany', in *Terrorists' use of the Internet: Assessment and Response,* edited by Maura Conway, Lee Jarvis, Orla Lehane, Stuart Macdonald, & Lella Nouri (Amsterdam, IOS Press, 2016).

Nowroz, M. O. 'Insider threats: detecting and controlling malicious insiders', in *New Threats and Countermeasures in Digital Crime and Cyber Terrorism,* edited by Maurice Dawson & Marwan Omar (Hershey, Information Science Reference, 2015).

O'Harrow Jr. R. *Zero day: the threat in cyberspace,* [Kindle version] (New York, Division Books, 2013).

Oakley, J. G. *Waging cyber war: technical challenges and operational constraints,* (Berkeley, Apress, 2019).

Omand, D. 'Learning from the secret past', in *Learning from the Secret Past: Cases in British Intelligence History,* edited by Robert Dover and Michael S. Goodman (Washington, Georgetown University Press, 2011).

Omand, D. 'Social media intelligence (SOCMINT)', *The Palgrave Handbook of Security, Risk, and Intelligence,* (London, Palgrave Macmillan, 2017).

Pincher, C. *The truth about dirty tricks: from Harold Wilson to Margaret Thatcher,* (London, Sidgwick & Jackson Ltd, 1990).

Prunckun H. *Counterintelligence theory and practice* [Google Play Books] (Lanham, MD, Rowman & Littlefield Publishers, 2012).

Quinlan, K. *The secret war between the wars: MI5 in the 1920s and 1930s* (Rochester, NY, The Boydell Press, 2014).

Redmond, P. ‘The challenges of counterintelligence’, in *Intelligence: The Secret World of Spies, an Anthology*, edited by Loch K. Johnson and James J. Wirtz (Oxford, Oxford University Press, 2011).

Richelson, J. T. *Wizards of Langley: inside the CIA’s Directorate of Science and Technology*, [Kindle version] (Oxford, Westview Press, 2002).

Rid, T. *Cyber war will not take place,* (Oxford, Oxford University Press, 2013).

Riley, P. R. ‘CIA and its discontents’, in *Intelligence and National Security: The Secret World of Spies,* edited by Loch K. Johnson & James J. Wirtz, (Oxford, Oxford University Press, 2008).

Roxburgh, A. *Strongman: Vladimir Putin and the struggle for Russia,* (London, I.B. Tauris, 2012).

Russel, R. L. *Sharpening strategic intelligence: why the CIA gets it wrong and what needs to be done to get it right,* [Kindle version] (New York, Cambridge University Press, 2007).

Sakwa, R. *Frontline Ukraine: crisis in the borderlands,* (London, I.B. Tauris, 2014).

Sayer, A. *Method in social science: a realist approach* (New York, Routledge, 1992).

Schmeidel, J. C. *Stasi: shield and sword of the party,* (London, Routledge, 2008).

Schneier, B. *Carry on sound advice from Schneier on Security,* (Indianapolis, John Wiley & Sons, Incorporated, 2013).

Schneier, B. *Data and Goliath: the hidden battles to collect your data and control your world,* [Kindle version] (New York, W. W. Norton & Company, 2015).

Scott, L. ‘Human intelligence’ in *Routledge Companion to Intelligence Studies,* edited by Robert Dover, Michael S. Goodman, and Claudia Hillebrand (Abingdon, Routledge, 2014).

Scott, L. ‘Oleg Penkovsky, British Intelligence, and the Cuban Missile Crisis’, in *Learning from the secret past: cases in British intelligence history,* edited by Robert Dover and Michael S. Goodman, (Washington, Georgetown University Press, 2011).

Shank, G. ‘Abduction’, in *The SAGE Encyclopedia of Qualitative Research Methods,* edited by Lisa M. Given (London, SAGE, 2008).

Sharma, A. ‘Cyber wars: a paradigm shift from means to end’, *The Virtual Battlefield: Perspectives on Cyber Warfare,* edited by Christian Czosseck & Kenneth Geers (Amsterdam, IOS Press, 2009).

Shavers, B. & Bair, J. *Hiding behind the keyboard: uncovering covert communication method with forensic analysis,* [Kindle version] (Cambridge MA, Syngress, 2016).

Sheffi, Y. *The power of resilience: how the best companies manage the unexpected,* (London, The MIT Press, 2015).

Shulsky, A. N. & Schmitt, G. J. *Silent warfare: understanding the world of intelligence,* (Washington, Brassey's, 2002).

Silva, E. D. 'Detecting individual-level deception in the digital age: The DETECT model', in *National security and counterintelligence in the era of cyber espionage,* edited by Eugenie de Silva (Hershey, Information Science Reference, 2016).

Sims, J. 'Defending adaptive realism: intelligence theory comes of age', *Intelligence theory,* edited by Peter Gill, Stephen Marrin, and Mark Phythian, (London, Routledge 2009).

Sims, J. E. & Gerber, B. 'The way ahead', *Vaults, Mirrors & Masks: Rediscovering U.S. counterintelligence,* edited by Jennifer E. Sims and Burton Gerber, (Washington, Georgetown University Press, 2009).

Sims, J. E. 'Democracies and counterintelligence: the enduring challenge', in *Vaults, mirrors & masks: Rediscovering U.S. counterintelligence,* edited by Jennifer E. Sims and Burton Gerber (Washington, Georgetown University Press, 2009).

Soldatov, A & Borogan, I. *The new nobility: The restoration of Russia's security state and the enduring legacy of the KGB,* (New York, Public affairs, 2010).

Soldatov, A. & Borogan, I. *The red web: the struggle between Russia's digital dictators and the new online revolutionaries,* [Kindle version] (New York, Public Affairs, 2015).

Stinissen, J. 'A legal framework for the cyber operations in Ukraine', in *Cyber War in Perspective: Russian Aggression Against Ukraine,* edited by Kenneth Geers, (Tallinn, NATO CCD COE, 2015).

Suvorov, V. *Soviet military intelligence*. (London, Hamilton, 1984).

Trahair, R. C. S *Encyclopedia of Cold War espionage,* (Westport, Greenwood Publishing Group, 2004).

Tucker, D. *End of intelligence: Espionage and state power in the information age,* (Palo Alto, Stanford University Press, 2014).

Valeriano, B. & Maness, R. C. *Cyber war versus cyber realities: cyber conflict in the international system,* (Oxford, Oxford University Press, 2015).

Wallace, R. & Melton, H. K. *C.I.A. manual of trickery and deception,* (London, Harper Collins, 2009).

Wallace, R., Melton, H. & Schlesinger, H. R. *Spycraft: inside the CIA's top secret spy lab,* (London, Bantam Press, 2008).

Wallace, R. 'A time for counterespionage', in *Vaults, Mirrors, & Masks: Rediscovering U.S. Counterintelligence,* (Washington, Georgetown University Press, 2008).

Walton, D. *Abductive reasoning,* (Tuscaloosa, The University of Alabama Press, 2005).

Warner, ‘The past and future of the intelligence cycle, in *Understanding the intelligence cycle*, edited by Mark Phythian, (London, Routledge, 2013).

Warner, M. *The rise and fall of intelligence: an international security history*, [Kindle version] (Washington, Georgetown University Press, 2014).

West, N. *Historical dictionary of Cold War counterintelligence*, (Plymouth, The Scarecrow Press, 2007).

West, N. *Historical dictionary of international intelligence*, (London, Rowman & Littlefield, 2015).

Wettering, F. L. ‘Counterintelligence: the broken triad’, in *Secret Intelligence: A Reader*, edited by Richrd J. Aldrich & Christopher Andrew (London, Routledge, 2009).

Wheeler, N. J. *Trusting enemies*, [Kinde version] (Oxford, Oxford University Press, 2018).

White, H. *The China choice: why we should share power*, (Oxford, Oxford University Press 2013).

Wise, D. *Tiger Trap: America’s secret spy war with China*, (Boston, Houghton Mifflin Harcourt, 2011).

Yahuda, M. *The international politics of the Asia-Pacific*, (Abingdon, Routledge, 2006).

Yong, D. *China’s struggle for status: the realignment*, (Cambridge, Cambridge University Press, 2009).

Young, S. *Minox: Marvel in miniature*, (Bloomington, AuthorHouse, 2000).

Zegart, A. *Flawed by design: the evolution of the CIA, JCS, and NSC*, (Stanford, Stanford University Press, 1999).

Zetter, K. *Countdown to zero day: Stuxnet and the launch of the world’s first digital weapon*, [Kindle version] (New York, Crown Publishers, 2014).

Memoirs and biographies

Ashley, C. *CIA spymaster* (Gretna, Pelican Publishing Company, 2004).

Bower, T. *The perfect English spy: Sir Dick White and the secret war 1935-90*, (London, Mandarin Paperbacks, 1996).

Cherkashin, V. & *Feifer, G. Spy handler: memoir of a KGB officer*, (New York, BasicBooks, 2005).

Clarridge, D. R & Diehl, D. *A spy for all seasons: my life in the CIA*, [Kindle version] (New York, Scribner, 1997).

Crumpton, H. A. *The art of intelligence: lessons from a life in the CIA's clandestine service*, (New York, Penguin Books, 2012).

Devine, J & Loeb, V. *Good hunting: An American spymaster's story,* (New York, Picador, 2014).

Duns, J. *Dead drop: the true story of Oleg Penkovsky and the Cold War's most dangerous operation*, [Kindle version] (London, Simon & Schuster, 2013).

Everett, J. A. *The making and breaking of an American spy*, (Durham CT, Strategic Book Group, 2011).

Garthoff, R. L. *A journey through the Cold War: a memoir of containment and coexistence,* (Washington, Brookings Institution Press, 2001).

Gordievsky, O. *Next stop execution: the autobiography of Oleg Gordievsky*, [Kindle version] (London, Endeavour Media, 2018).

Hoffman, D. E. *The billion dollar spy: a true story of Cold War espionage and betrayal*, [Kindle version] (London, Icon Books, 2017).

Holm, R. *The craft we chose: my life in the CIA*, (Oakland, Mountain Lake Press, 2011).

Lett, B. *SOE's mastermind: the authorised biography of Major General Sir Colin Gubbins*, (Barnsley, Pen & Sword Books, 2016).

MacIntyre, B. *The spy and the traitor; the greatest espionage story of the Cold War*, [Kindle version] (London, Penguin Books, 2019).

Mahle, M. B. *Denial and deception: an insider's view of the CIA* (New York, Public affairs, 2005).

Mendez, A. J. & McConnell, M. *The master of disguise: my secret life in the CIA*, [Kindle version] (New York, Harper Collins, 2007).

Penkovsky, O. *The Penkovsky papers: the Russian who spied for the West*, (London, Collins, 1967).

Sager, J. *Uncovered: my half-century with the CIA*, (Bloomington, WestBow Press, 2013).

Sheymov, V. *Tower or secrets: a real life spy thriller*, [Kindle version] (New York, Harper, 2012).

Tomlinson, R. *The big breach: from top secret to maximum security*, (Edinburgh, Cutting Edge, 2001).

Weiser, B. *A secret life: the Polish officer, his covert mission, and the price he paid to save his country*, [Kindle version] (New York, Perseus, 2004).

Wise, D. *Spy: the inside story of how the FBI's Robert Hanssen betrayed America*, (New York, Random House, 2002)

Wright, P. & Greenglass, P. *Spycatcher,* (New York, Viking Penguin Inc, 1987).

Journals

Aldrich, J. R. 'Intelligence, Anglo-American Relations and the Suez Crisis, 1956', *Intelligence and National Security,* 9:3, 2008, pp. 544-554.

Allison, R. 'Russia and Syria: explaining alignment with a regime in crisis', *International Affairs,* 89:4, 2013, pp. 795-823.

Anderson, J. 'The HUMINT offensive from Putin's Chekist state', *International Journal of Intelligence and Counterintelligence,* 20:2, 2007, pp. 258-316.

Bagley, T. 'Ghosts of the spy wars: a personal reminder to interested parties', *International Journal of Intelligence and Counterintelligence,* 28:1, 2015, pp. 1-37.

Bateman, A., 'The political influence of the Russian security services', *The Journal of Slavic Military Studies,* 27:3, 2014, pp. 380-403.

Beeson, M. & Li, F. 'What consensus? Geopolitics and policy paradigms in China and the United States', *International Affairs,* 91:1, 2015, pp. 93-109.

Benes, L. 'OSINT, new technologies, education: expanding opportunities and threats. A new paradigm', *Journal of Strategic Security,* 6:3, 2013, pp. 4-37.

Ben-Haim, Y. 'Positivism and its limitations for strategic intelligence: a non-constructivist info-gap critique', *Intelligence and National Security,* 33:6, 2018, pp. 904-917.

Ben-Ze'ev, A. 'Privacy, emotional closeness, and openness in cyberspace', *Computers in Human Behaviour,* 19:4, 2003, pp. 451-467.

Berkowitz, B. 'The DI and "IT": Failing to keep up with the information revolution', *Studies in Intelligence,* CIA, 74:1, 2003.

Bimfort, M. T. 'A definition of intelligence', *Studies in Intelligence,* CIA, 2:2, 1958.

Brown, I. & Korff, D. 'Foreign surveillance: law and practice in a global digital environment', *European Human Rights Law Review,* 2014, pp. 243-251.

Brown, I. 'Data protection: The new technical and political environment', *Computers & Law,* 20:6, 2010, pp. 1-6.

Burkett, R. 'Rethinking an old approach: an alternative framework for agent recruitment: from MICE to RASCLS', *Studies in Intelligence,* CIA, 57:1, 2013.

Bury, J. ‘Finding needles in a haystack: the Eastern Bloc’s counterintelligence capabilities’, *International Journal of Intelligence and Counterintelligence,* 25:4, 2011, pp. 727-770.

Bury, J. ‘From the archives: the U.S. and West German agent radio ciphers’, *Cryptologia,* 31:4, 2007, pp. 343-357.

Bury, J. ‘Project Kalina: the Lotos operation conundrum', *Cryptologia,* 36:2, 2012, pp. 119-128.

Busynski, L. ‘The South China Sea: oil, maritime claims, and U.S. – China strategic rivalry’, *The Washington Quarterly,* 35:2, 2012, pp. 139-156.

Butrimas, V. ‘National security and international policy challenges in a post Stuxnet world’, *Lithuanian Annual Strategic Review,* 12, 2014, pp. 11-31.

Caddell, J. Jr & Caddell, J. Sr. ‘Historical case studies in intelligence education: best practices, avoidable pitfalls’, *Intelligence and National Security,* 32:7, 2017, pp. 1-16.

Chen, R. ‘A critical analysis of the U.S. “pivot” towards the Asia-Pacific: how realistic is neo-liberalism?, *Connections,* 12:3, 2013, pp. 39-62.

Cross, S. ‘NATO-Russia security challenges in the aftermath of Ukraine conflict: managing Black Sea security and beyond’, *Southeast European and Black Sea Studies,* 15:2, 2015, pp. 151-177.

Cyr, B, Horn, W., Miao, D., Specter, M. ‘Security analysis of wearable fitness devices (Fitbit)’ *Massachusetts Institute of Technology (MIT),* 2014, 1-14.

Delanoe, I., ‘After the Crimean crisis: towards a greater Russian maritime power in the Black Sea’, *Southeast European and Black Sea Studies,* 2014.

Demarest, G. B. ‘Espionage in international law’, *Denver Journal of International Law and Policy,* 24:2, 1996, pp. 321-348.

Dian, M. ‘The pivot to Asia, Air-Sea Battle and contested commons in the Asia region’, *The Pacific Review,* 28:2, 2015, pp. 237-257.

Easter, D. ‘Soviet Bloc and Western bugging of opponents’ diplomatic premises during the early Cold War’, *Intelligence and National Security,* 3:1, 2016, pp. 28-48.

Ehrman, J. ‘What are we talking about when we talk about counterintelligence?’, *Studies in Intelligence,* CIA, 53:2, 2009.

Farwell, J. P. & Rohozinski, R., ‘Stuxnet and the future of cyber war’, *Survival,* 53:1, 2011.

Fischer, B. B. ‘Double troubles: the CIA and double agents during the Cold War’, *International Journal of Intelligence and Counterintelligence,* 29:1, 2016, pp. 48-74.

Fischer, B. B. ‘Fictitious spies and fake history’, *International Journal of Intelligence and Counterintelligence,* 33:1, 2019.

Fischer, B. B. ‘The man who wasn’t there’, *International Journal of Intelligence and Counterintelligence,* 30:1, 2017, pp. 30-52.

Freedman, L. ‘Ukraine and the art of limited war’, *Global Politics and Strategy,* 56:6, 2014, pp. 7-38.

Friedberg, A. ‘The future of US-China relations: Is conflict inevitable?’ *International Security,* 30:2, 2005, pp. 7-45.

Fripp, W. ‘The hacked world order: how nations fight, trade, maneuver, and manipulate in the digital age’, *Book Review, Intelligence and National Security,* 33:4, 2018, pp. 623-626.

Gainous, J. Wagner, K. M. & Ziegler, C. E. ‘Digital media and political opposition in authoritarian systems: Russia’s 2011 and 2016 Duma election’, *Democratization,* 25:2, 2016, pp. 209-226.

Garfinkel, S. L. ‘The cybersecurity risk’, *Communications of the ACM,* 55:6, 2012, 29-32.

Garrie, D. & Byhovsky, I. ‘Privacy and data protection in Russia’, *Journal of Law and Cyber Warfare,* 5:2, 2017, pp. 235-253.

Gartzke, E. & Lindsay, J. R. ‘Weaving tangled webs: offense, defense, and deception in cyberspace’, *Security Studies,* 24:2, 2015, pp. 316-348.

Gioe, D. V. ‘Cyber operations and useful fools: the approach of Russian hybrid intelligence’, *Intelligence and National Security,* 33:7, 2018, pp. 954.973.

Goldstein, A. ‘First things first: the pressing danger of crisis instability in U.S. – China relations’, *International Security,* 37:4, 2013, pp. 49-89.

Hegghammer, T. ‘Interpersonal trust on Jihadi internet forums’, *Norwegian Defence Research Establishment,* 2014.

Hill, J. F. ‘The growth of data localization post-Snowden: analysis and recommendations for U.S. policymakers and business leaders’, *The Hague Institute for Global Justice, Conference on the Future of Cyber Governance,* 2014, pp. 1-34.

Hughes, R. G. & Chen, K. “The enlightened prince and the wide general’: the history of Chinese intelligence’, *Intelligence and National Security,* 34:7, 2018, pp. 1085-1091.

Inkster, N. ‘Chinese intelligence in the cyber age’, *Global politics and strategy,* 55:1, 2013, pp. 45-66.

Inkster, N. ‘Intelligence agencies and the cyber world’, *Strategic Survey,* (2012), pp. 33-74.

Ivan, A. L, Iov, C. A., Lutai, R. C. & Grad, M. N. ‘Social media intelligence: opportunities and limitations’, *CES Working Papers,* 7:2, 2015, 505-510.

Jang-Jaccard, J. ‘A survey of emerging threats in cybersecurity’, *Journal of Computer and System Sciences,* 80:5, 2014, pp. 973-993.

Johnson, L. ‘Evaluating “HUMINT”: the role of foreign agents in U.S. security’, *Comparative Strategy,* 29:4, 2010, pp. 308-332.

King, Pan, & Roberts, ‘How the Chinese government fabricates social media posts for strategic deception, not engaged argument’, *American Political Science Review,* 111:3, 2017, pp. 484-501.

Kissinger, H. ‘The future of U.S.-Chinese relations’, *Foreign Affairs,* 91:2, 2012, pp. 44-55.

Kringen, J. A. ‘Keeping watch on the world: rethinking the concept of global coverage in the US Intelligence Community’, *Studies in Intelligence,* CIA, 59:3, 2015.

Kroenig, M. ‘Facing reality: getting NATO read for a new Cold War’, *Survival; Global Politics and Strategy,* 57:1, 2015, pp. 49-70.

Landau, S. ‘Making sense from Snowden: what’s significant in the NSA surveillance revelations’, *IEEE Security & Privacy,* 11:4, 2013, pp. 54-63.

Lawson, H. M. & Leck, K. ‘Dynamics of Internet dating’, *Social Science Computer Review,* 24:2, 2006, pp. 189-208.

Loleski, S. ‘From cold to cyber warriors: the origins and expansion of NSA’s Tailored Access Operations (TAO) to Shadow Brokers’, *Intelligence and National Security,* 34:1, 2018, pp. 112-128.

Lord, J. ‘Undercover under threat: Cover identity, clandestine activity, and covert action in the digital age’, *International Journal of Intelligence and Counterintelligence,* 28:4, 2015, pp. 666-691.

MacFarlane, N. & Menon, A. ‘The EU and Ukraine’, *Survival: Global Politics and Strategy,* 56:3, 2014, pp. 95-101.

Macrakis, K. ‘Technophilic hubris and espionage styles during the Cold War’, *Isis,* 101:2, 2010, pp. 378-385.

Madianou, M. & Miller, D. ‘Polymedia: towards a new theory of digital media in interpersonal communication’, *International Journal of Cultural Studies,* 16:2, 2012, pp. 169-187.

Mattis, P. ‘The Analytic challenge of understanding Chinese intelligence services’, *Studies in Intelligence,* CIA, 56:3, 2012, pp. 47-55.

Mattis, P. ‘Beyond spy vs. spy: the analytic challenge of understanding Chinese intelligence services’, *Studies in Intelligence,* CIA, 56:3, 2012.

McDevitt, M. ‘The East China Sea: the place where Sino-U.S. conflict could occur’, *American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy,* 36:2, 2014, pp. 100-110.

McKenna, K. Y. A., Green, A. S. & Gleason, M. E. J. 'Relationship formation on the Internet: what's the big attraction?', *Journal of Social Issues,* 58:1, 2002, pp. 9-31.

Michalevsky, Y., Schulman, A., Veerapandian, G. A. & Boneh, D. 'PowerSpy: Location tracking using mobile device power analysis', *24th Usenix Security Symposium,* 2015, pp. 785-800.

Moran, C. 'The pursuit of intelligence history: methods, sources, and trajectories in the United Kingdom', *Studies in Intelligence,* CIA, 55:2, 2011.

Næss, P. 'Prediction, regressions and critical realism', *Journal of Critical Realism,* 3:1, 2004, pp. 133-164.

Nodia, G. 'The revenge of geopolitics', *Journal of Democracy,* 25:4, 2014, pp. 139-150.

Norval, A. & Prasopoulou, E. 'Public faces? A critical exploration of the diffusion of face recognition technologies in online social networks', *New Media & Society,* 19:4, 2017, pp. 1-18.

Omand, D. Bartlett, J. Miller, C. 'Introducing social media intelligence (SOCMINT)', *Intelligence and National Security,* 27:6, 2012, pp. 801-823.

Ottis, R., Lorents, P. 'Cyberspace: definition and implications.' *Proceedings of the 5th International Conference on Information Warfare and Security,* 2010, pp. 267-270.

Pool, P. 'War of the cyber world: the law of cyber warfare', *International Lawyer,* 47:2, 2013, pp. 299-324.

Royden, B. G. 'Tolkachev, a worthy successor to Penkovsky', *Studies in Intelligence,* CIA, 47:3, 2008.

Runciman, B. 'A bigger haystack…', *ITNow,* 54:2, 2012, pp. 36-37.

Rutland, P. & Middletown, CT. 'The impact of sanctions on Russia', *Russian Analytical Digest,* 157, 2014, pp. 1-7.

Sano, J. 'The changing shape of HUMINT', *Intelligencer,* 21:3, 2015, pp. 77-80.

Sargsyan, T. 'Data localization and the role of infrastructure for surveillance, privacy, and security', *International Journal of Communication,* 2016, pp. 2221-2237.

Schnader, J. 'Alexa, are you a foreign agent? Confronting the risk of foreign intelligence exploitation of private home networks, home assistants, and connectivity in the security clearance process', *Richmond Journal of Law & Technology,* 25:4, 2019, pp. 1-63.

Scott, L. & Hughes, G. 'Intelligence, crises and security: lessons from history?', *Intelligence and National Security,* 21:5, 2006, pp. 653-674.

Scott, L. & Jackson, P. 'The study of intelligence in theory and practice', *Intelligence and National Security,* 19:2, 2004, pp. 139-169.

Scott, L. ‘Espionage and the cold war: Oleg Penkovsky and the Cuban missile crisis’, *Intelligence and National Security,* 14:3, 1999, pp. 23-47.

Selby, J ‘Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?’, *International Journal of Law and Information Technology,* 25:3, 2017, pp. 213-232.

Sherman, L. E., Michikyan, M. & Greenfield, P. M. ‘The effects of text, audio, video, and in-person communication on bonding between friends’, *CyberPsychology,* 7:2, 2013, pp. 1-13.

Soldatov, A. & Borogan, I. ‘Russia’s surveillance state’, *World Policy Journal*, 30:3, 2013, pp. 23-30.

Steinberg, J. & O’Hanlon, M. ‘Keep hope alive: how to prevent U.S. – Chinese relations from blowing up’, *Foreign Affairs,* 93:4, 2014, pp. 107-117.

Stevens, T. ‘Security and Surveillance in Virtual Worlds: Who Is Watching the Warlocks and Why?’, *International Political Sociology*, 9, 2015, pp. 230-247.

Stoddart, K. ‘Live free or die hard: U.S.-UK cybersecurity policies.’ *Political Science Quarterly,* 131:4, 2016, pp. 803-842.

Sukhankin, S. ‘Russia on the verge of a ‘cyber purge?’’, *The Jamestown Foundation*, 14:16, 2017. Available at: https://jamestown.org/program/russia-verge-cyber-purge/ [accessed 12 May 2020].

Suler, J. ‘The online disinhibition effect’, *Cyberpsychology & Behavior,* 7:3, 2004, pp. 321-326.

Tal, A. & Siman-Tov, D. ‘HUMINT in the cybernetic era: gaming in two worlds’, *Military and Strategic Affairs,* 7:3, 2015, pp. 93-102.

Timmermans, S. & Tavory, I. ‘Theory construction in qualitative research: from grounded theory to abductive analysis’, *Sociological Theory,* 30:3, 2012, pp. 167-186.

Van Cleave, M. ‘Strategic counterintelligence: what is it and what should we do about it?’ *Studies in Intelligence,* 51:2, 2006, pp. 1-22.

Verble, J. ‘The NSA and Edward Snowden: surveillance in the 21st Century’, *ACM SIGCAS Computers and Society,* 44:3, 2014, pp. 14-20.

Vogel, R. ‘Insider threats: The FBI and the Robert Hanssen espionage case’, *Journal of the AIPIO* (Australian Institute of Professional Intelligence Officers), 22:1, 2014, pp. 3-19.

Warner, M. ‘Reflections on technology and intelligence systems’ *Intelligence and National Security,* 27:1, 2012, pp. 133-153.

Wendt, A. E. ‘The agent-structure problem in international relations theory’, *International Organization*, 41:3, 1987, pp. 335-370.

Wilder, U. M. ‘The psychology of espionage and leaking in the digital era’, *Studies in Intelligence, CIA*, 61:2, 2017.

Winter, L. & Lindskog, S. ‘How the Great Firewall of China is blocking Tor’, *2nd USENIX Workshop on Free and Open Communications on the Internet,* 2012, pp. 1-7.

Wippl, J. W. ‘The CIA and Tolkachev vs. the KGB/SVR and Ames: a comparison’, *International Journal of Intelligence and Counterintelligence*, 23:4, 2010, pp. 636-646.

Wynn, Jr. D. & Williams, C. K. ‘Principles for conducting critical realist case study research in information systems’, *MIS Quarterly,* 36:3, 2012, pp. 787-810.

Zhao, S. ‘A new model of big power relations? China-US strategic rivalry and balance of power in the Asia-Pacific’, *Journal of Contemporary China,* 24:93, pp. 377-397.

Official online resources

‘United States of America v. Monica Elfriede Witt, Mojtaba Masoumpour, Behzad Mesri, Hossein Parvar, and Mohamad Paryar’*, Department of Justice,* 2018.

Cabinet Office (1 November 2016) Britain’s cyber security bolstered by world-class strategy. Available at: https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy [accessed 10 January 2018].

Cabinet Office (2010) National Intelligence Machinery. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61808/nim-november2010.pdf p.8 [accessed 1 March 2018].

Cabinet Office (925 June 2018) Minimum cyber security standard. Available at: https://www.gov.uk/government/publications/the-minimum-cyber-security-standard [accessed 25 May 2020]

Cabinet Office (November 2011) The UK cyber security strategy. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf [accessed 31 October 2017].

CCDCOE - Cyber definitions. Available at: https://ccdcoe.org/cyber-definitions.html [accessed 31 October 2017]

CIA - Contact CIA. Available at: https://www.cia.gov/cgi-bin/forlang_form.cgi [accessed 15 September 2020].

CIA – Directorate of Operations (formerly known as the Clandestine Service). Available at: https://www.cia.gov/careers/opportunities/clandestine/index.html [accessed 1 March 2018].

CIA - History of the CIA. Available at: https://www.cia.gov/about-cia/history-of-the-cia [accessed 1 March 2018].

CIA (14 February 2018) Romeo spies. Available at: https://www.cia.gov/news-information/featured-story-archive/2018-featured-story-archive/romeo-spies.html [accessed 20 July 2020].

CIA (18 September 2015) Deputy Director Cohen delivers remarks on CIA of the future at Cornell University. Available at: https://www.cia.gov/news-information/speeches-testimony/2015-speeches-testimony/deputy-director-cohen-delivers-remarks-on-cia-of-the-future-at-cornell-university.html [accessed 10 January 2018]

CIA (2013) INTelligence: human intelligence. Available at: https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-human-intelligence.html [accessed 1 January 2017].

CIA (2013) The capture and execution of Colonel Penkovsky, 1963. Available at: https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/colonel-penkovsky.html [accessed 1 January 2018].

CIA (21 January 2011) A look back … CIA asset Popov arrest. Available at: https://www.cia.gov/news-information/featured-story-archive/2011-featured-story-archive/pyotr-popov.html [accessed 14 August 2017].

CIA (29 March 2016) The billion dollar spy: a true story of Cold War espionage and betrayal, reviewed by Nicholas Dujmovic. Available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-60-no-1/the-billion-dollar-spy.html [accessed 12 January 2021].

CIA (7 May 2019) CIA's latest layer: an Onion site. Available at: https://www.cia.gov/news-information/press-releases-statements/2019-press-releases-statements/ciagov-over-tor.html [accessed 15 September 2020].

CIA (22 December 2016) Restrictions on foreign travel in the USSR: Assessing recent changes. Available at: https://www.cia.gov/library/readingroom/docs/CIA-RDP07C00121R001000280001-8.pdf [accessed 1 January 2018].

Department of Defense (2016) Summary of the 2018 National Defense Strategy of the United States of America: sharpening the American military's competitive edge. Available at: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf [accessed 1 March 2018].

Department of Homeland Security – Explore terms: a glossary of common cybersecurity terminology. Available at: https://niccs.us-cert.gov/about-niccs/glossary [accessed 1 December 2018].

FBI - Ghost stories: Russian Foreign Intelligence Service (SVR) Illegals. Available at: https://vault.fbi.gov/ghost-stories-russian-foreign-intelligence-service-illegals [accessed 31 November 2017].

FBI – The insider threat: an introduction to detecting and deterring an insider spy. Available at: https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view [accessed 10 January 2018].

FBI (23 March 2010) The cyber threat: who's doing what to whom?'. Available at: https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom [accessed 1 March 2018].

FBI (27 September 2017) Current threats to the homeland. Available at: https://www.fbi.gov/news/testimony/current-threats-to-the-homeland [accessed 10 January 2018].

FBI, (19 May 2014) Combating state-sponsored cyber espionage, https://www.fbi.gov/news/speeches/combating-state-sponsored-cyber-espionage [accessed 23 February 2018].

Finklea, K., Christensen, M. D., Fischer, E. A., Lawrence, S. V. & Theohary, C. A. Cyber intrusion into U.S. Office of Personnel Management: In brief. Congressional Research Service, 2015. Available at: https://fas.org/sgp/crs/natsec/R44111.pdf [accessed 31 November 2017].

Fischer, E. A. 'The Internet of Things: Frequently Asked Questions', Congressional Research Service, 2015. Available at: http://www.fas.org/sgp/crs/misc/R44227.pdf [accessed 23 May 2020].

Foreign & Commonwealth Office (22 October 2015) UK – China joint statement on building a global comprehensive strategic partnership for the 21st Century. Available at: https://www.gov.uk/government/news/uk-china-joint-statement-2015 [accessed 31 October 2017].

Galeotti, M. (12 May 2017) Russian intelligence is at war, NATO Review. Available at: https://www.nato.int/docu/review/articles/2017/05/12/russian-intelligence-is-at-political-war/index.html [accessed 12 September 2020].

Galeotti, M. 'Putin's Hydra: inside Russia's intelligence services', European Council on Foreign Relations, 2016. Available at: http://www.ecfr.eu/page/-/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf [accessed 31 November 2017].

Gov.UK - UK Visas and Immigration. Available at: https://www.gov.uk/government/publications/exempt-exm/exempt-exm [accessed 11 January 2018].

Gov.UK (21 October 2013) Think before you share online. Available at: https://www.gov.uk/guidance/think-before-you-share [accessed 12 May 2020].

HM Government (November 2015) National security strategy and strategic defence and security review 2015, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf [accessed 31 October 2017].

HM Treasury (17 November 2015) Chancellor's speech to GCHQ on cyber security. Available at: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security [accessed 10 January 2018].

Home Office (December 2017) Intelligence services' retention and use of bulk personal datasets. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668933/Draft_BPD-_Intelligence_Services__Retention_and_Use_of_Bulk_Personal_Datasets.pdf [accessed 1 March 2018].

Homeland Security – EINSTEIN. Available at: https://www.dhs.gov/einstein [accessed 1 March 2018].

ICS-CERT (25 February 2016) Cyber-attack against Ukrainian critical infrastructure. Available at: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 [accessed 31 November 2017].

Intelligence and Security Committee of Parliament (20 December 2017) Annual report 2016-2017. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727949/ISC-Annual-Report-2016-17.pdf [accessed 11 January 2018].

Intelligence and Security Committee of Parliament, 'Privacy and security: a modern and transparent legal framework', House of Commons, 2015.

Kont, M., Pihelgas, M., Wojtkowiak, J., Osula, A-M. & Trinberg, L. 'Insider threat detection study', NATO Cooperative Cyber Defence Centre of Excellence, 2018

Mandiant (February 2013) APT1 Exposing one of China's cyber espionage units. Available at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf [accessed 31 October 2017].

Ministry of Defence (22 October 2012) Using social media – a guide for military personnel. Available at: https://www.gov.uk/government/publications/using-social-media-a-guide-for-military-personnel [accessed 1 January 2018].

O'Rourke, R. 'China naval modernization: Implications for U.S. Navy capabilities – backing and issues for Congress', Congressional Research Service, 2017.

Office of the Director of National Intelligence – Know the risk raise your shield: NSCS awareness materials. Available at: https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-awareness-materials [accessed 15 March 2017].

Office of the Director of National Intelligence – Members of the IC. Available at: https://www.dni.gov/index.php/what-we-do/members-of-the-ic [accessed 1 March 2018].

Office of the Director of National Intelligence – What we do. Available at: https://www.dni.gov/index.php/what-we-do [accessed 1 March 2018].

Office of the Director of National Intelligence (2017) Worldwide threat assessment of the US Intelligence Community. Available at: https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf [accessed 15 January 2018]

Office of the Director of National Intelligence (2018) Statement for the record: worldwide threat assessment of the US intelligence community. Available at: https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1845-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community [accessed 12 June 2018].

Office of the Director of National Intelligence (6 January 2017) Background to "Assessing Russian activities and intentions in recent US elections": The analytical process and cyber incident attribution." Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf [accessed 31 November 2017].

Office of the Director of National Intelligence (9 February 2016) Worldwide threat assessment of the US intelligence community. Available at: https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf [accessed 31 November 2017].

Office of the National Counterintelligence Executive (2011) Foreign spies stealing US economic secrets in cyberspace. Available at: https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf [accessed 31 October 2017].

Office of the National Counterintelligence Executive (3 November 2011) Foreign spies stealing US economic secrets in cyberspace. Available at: https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf [accessed 31 October 2017].

Official Internet Resources of the President of Russia (16 February 2017) Meeting of Federal Security Service Board. Available at: http://en.kremlin.ru/events/president/news/53883 [accessed 24 October 2017].

Olson, J. M. (14 April 2007) 'A never-ending necessity: the ten commandments of counterintelligence', *CIA*. Available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/fall_winter_2001/article08.html [accessed 17 July 2016].

OPM.gov (9 July 2015) OPM announces steps to protect federal workers and others from cyber threats. Available at: https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/ [accessed 1 March 2017]

Parliament (25 March 2016) Supplementary written evidence submitted by Dr Victor Madeira. Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/russia-implications-for-uk-defence-and-security/written/31103.pdf [accessed 2 January 2018].

President of Russia (9 February 2015) Interview to Al-Ahram daily. Available at: http://en.kremlin.ru/events/president/news/47643 [accessed 30 October 2017].

Reed, M. G. & Syverson, P. F. 'Onion routing', Center for High Assurance Computer Systems, Naval Research Laboratory, 1999.

SIS – Contact us. Available at: https://www.sis.gov.uk/contact-us-form.html?lan=en [accessed 20 September 2017].

SIS – Our history. Available at: https://www.sis.gov.uk/our-history.html [accessed 1 March 2018].

The Ministry of Foreign Affairs of Russia (3 December 2014) About the new requirement for foreign nationals and stateless persons to provide their biometric data when applying for Russian visas on the territory of the United Kingdom. Available at: https://www.rusemb.org.uk/consnews/29 [accessed 11 January 2018].

The United States Department of Justice (19 May 2014) U.S. charges five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization for commercial advantage. Available at: https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor [accessed 31 October 2017]

The White House (1 February 2015) National security strategy. Available at: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf [accessed 31 October 2017].

The White House (29 December 2016) Statement by the President on actions in response to Russian malicious cyber activity and harassment. Available at: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity [accessed 10 January 2018].

The White House (December 2017) National Security Strategy. Available at: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf [accessed 2 December 2018].

U.S. – China Economic and Security Review Commission (16 November 2016) Annual report to Congress. Available at: https://www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%202%2C%20Section%203%20-%20China%27s%20Intelligence%20Services%20and%20Espionage%20Threats%20to%20the%20United%20States.pdf [accessed 10 January 2018]. Teabeamet Estonian Information Board (2017) ‘International security and Estonia’. Available at: https://www.valisluureamet.ee/pdf/2017-en-c482143c.pdf [accessed 24 October 2017].

U.S. Cyber Command - U.S. Cyber Command History. Available at: https://www.cybercom.mil/About/History/ [accessed 23 May 2020].

U.S. Department of Defense (18 August 2017) DoD initiates process to elevate U.S. Cyber Command to unified combatant command. Available at: https://www.defense.gov/Explore/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/ [accessed 34 May 2020].

United States of America v. Evgeny Buryakov, a/k/a “Zhenya,”, Igor Sporyshev, and Victor Podobnyy, Department of Justice, 2015.

United States of America v. Jun Wei Yeo, also known as Dickson Yeo, United States District Court for the District of Columbia, 2020.

Van Cleave, M. (9 June 2016) Chinese intelligence operations and implications for U.S. national security, U.S. - China Economic and Security Review Commission. Available at: http://www.uscc.gov/sites/default/files/Michelle%20Van%20Cleave_Written%20Testimony060916.pdf [accessed 31 November 2017].

White House (2017) National Security Strategy. Available at: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf [accessed 1 February 2018].

Wilson, C. CRS report for Congress: Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for Congress, Congressional Research Service, 2008. Available from https://www.fas.org/sgp/crs/terror/RL32114.pdf, [accessed 31 October 2017].

Unofficial online resources

Bauer, M., Lee-Makiyama, H. & Marel, E. V. D. 'Data localisation in Russia: A self-imposed sanction', European Centre for International Political Economy, 6, 2015.

Belfer Center (July 2009) Congressional oversight of the Intelligence community. Available at: https://www.belfercenter.org/publication/congressional-oversight-intelligence-community [accessed 1 March 2018].

Bellingcat (13 November 2015) Artillerymen of Russia's 136th Motorized Infantry Brigade in the Donbass. Available at: https://www.bellingcat.com/news/uk-and-europe/2015/11/13/136-brigade-in-donbass/ [accessed 25 October 2019].

Bellingcat (16 November 2018) Spies without borders – how the FSB infiltrated the international visa system. Available at: https://www.bellingcat.com/news/uk-and-europe/2018/11/16/spies-without-borders-fsb-infiltrated-international-visa-system/ [accessed 10 July 2019].

Bellingcat (19 June 2019) Identifying the separatists linked to the downing of MH17. Available at: https://www.bellingcat.com/news/uk-and-europe/2019/06/19/identifying-the-separatists-linked-to-the-downing-of-mh17/ [accessed 25 October 2019].

Bellingcat (20 September 2018) Skripal suspects confirmed as GRU operatives: prior European operations disclosed. Available at: https://www.bellingcat.com/news/uk-and-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-european-operations-disclosed/ [accessed 10 July 2019].

Carnegie (30 May 2019) The encryption debate in China. Available at: https://carnegieendowment.org/2019/05/30/encryption-debate-in-china-pub-79216 [accessed 12 July 2020].

Castro, D. & McQuinn, A. (9 June 2015) 'Beyond the USA Freedom Act: How U.S. surveillance still subverts U.S. competitiveness', *Information Technology & Innovation Foundation*. Available at: http://www2.itif.org/2015-beyond-usa-freedom-act.pdf [accessed 12 January 2021].

Crypto Museum – RS-804: US satellite spy radio set. Available at: https://www.cryptomuseum.com/spy/rs804/index.htm [accessed 12 March 2019].

Electronic Frontier Foundation (19 July 2016) Russia asks for the impossible with its new surveillance laws. Available at: https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws [accessed 21 July 2020].

FBI (1 November 2016) A primer on DarkNet marketplaces: what they are and what law enforcement is doing to combat them. Available at: https://www.fbi.gov/news/stories/a-primer-on-darknet-marketplaces [accessed 22 September 2020].

FireEye (21 June 2016) Redline drawn: China recalculates its use of cyber espionage. Available at: https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf [accessed 2 November 2017].

FireEye (27 October 2014) APT28: A window into Russia's cyber espionage operations? Available at: https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html [accessed 31 November 2017].

Freedom House (1 November 2017) Freedom of the press 2017, China. Available at: https://freedomhouse.org/report/freedom-press/2017/china [accessed 10 January 2018]

FrontLine - Digital security and privacy for human rights defenders. Available at: https://www.frontlinedefenders.org/en/digital-security-resources [accessed 23 June 2017].

Green, M. (16 Jan 2018) Apple in China: Who holds the keys?, Cryptography Engineering. Available at: https://blog.cryptographyengineering.com/about-me/ [accessed 21 January 2018].

Human Rights Watch (15 May 2017) China: Police DNA Database Threatens Privacy. Available at: https://www.hrw.org/news/2017/05/15/china-police-dna-database-threatens-privacy [accessed 18 January 2021].

Human Rights Watch (18 June 2020) Russia: growing internet isolation, control, censorship. Available at: https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship [accessed 10 September 2020].

Human Rights Watch (2 October 2020) Russia expands facial recognition despite privacy concerns. Available at: https://www.hrw.org/news/2020/10/02/russia-expands-facial-recognition-despite-privacy-concerns [accessed 21 October 2020].

Interagency OPSEC support staff (June 2004) Intelligence Threat Handbook, *Federation of American Scientists.* Available at: http://fas.org/irp/threat/handbook/ [accessed 09 January 2021].

Medium (4 October 2019) Using Tor in China. Available at: https://medium.com/@phoebecross/using-tor-in-china-1b84349925da [accessed 20 September 2020].

Omand, D. 'Understanding digital intelligence and the norms that might govern it', *Global Commission on Internet Governance*, 8, 2015.

Pifer, S. 'Will Ukraine join NATO? A course for disappointment', Brookings 25 July 2017. Available at https://www.brookings.edu/blog/order-from-chaos/2017/07/25/will-ukraine-join-nato-a-course-for-disappointment/ [accessed 30 October 2017].

Reporters Without Borders – Russia: Stifling atmosphere for independent journalists. Available at: https://rsf.org/en/russia [accessed 10 January 2018].

Ryan, T. (2010) Getting in bed with Robin Sage, *BlackHat USA*. Available at: https://www.privacywonk.net/download/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf [accessed 13 January 2021].

Scan-X Security ltd - Security scanners, X-ray scanners & people screening. Available at: http://www.scanxsecurity.com/people-screening/ [accessed 21 August 2020].

Scott, J., Spaniel, D. & Schumacher, C. 'Preparing the battlefield: The coming espionage culture post OPM breach', *Institute for Critical Infrastructure,* 2015.

Security in-a-box - Remain anonymous and bypass censorship on the Internet. Available at: https://securityinabox.org/en/guide/anonymity-and-circumvention/ [accessed 22 December 2018].

Security In-a-Box - Tor browser for Windows – online anonymity and censorship circumvention. Available at: https://securityinabox.org/en/guide/torbrowser/windows/ [accessed 23 July 2020].

Simms – Levels of encryption. Available at: https://www.simms.co.uk/tech-talk-2/levels-of-encryption/ [accessed 10 January 2018].

Soldatov, A. & Borogan, I. (15 November 2011) A face in the crowd: the FSB is watching you!, *Open Democracy*. Available at: https://www.opendemocracy.net/od-russia/andrei-soldatov-irina-borogan/face-in-crowd-fsb-is-watching-you [accessed 11 January 2018].

Spy Museum – Moscow Rules. Available at: https://www.spymuseum.org/exhibition-experiences/online-exhibits/argo-exposed/moscow-rules/ [accessed 1 December 2017].

Steele, C. (11 January 2017) US Presidential election: Republican candidate Donald Trump's activities in Russia and compromising relationship with the Kremlin, Cryptome. Available at: https://cryptome.org/2017/01/Steele-Trump.pdf [accessed 31 November 2017].

The Jamestown Foundation (7 May 2014) Virtual espionage challenges Chinese counterintelligence. Available at: https://jamestown.org/program/virtual-espionage-challenges-chinese-counterintelligence/ [accessed 1 January 2017].

The Jamestown Foundation (February 9 2017) Russia on the verge of a 'cyber purge?' Available at: https://jamestown.org/program/russia-verge-cyber-purge/ [accessed 4 January 2020].

Tor – Directly connecting users, 2017-01-01 to 2018-01-01. Available at: https://metrics.torproject.org/userstats-relay-country.html?start=2017-01-01&end=2018-01-01&country=all&events=off [accessed 1 February 2018]

Tor - Tor: overview. Available at: https://2019.www.torproject.org/about/overview.html.en [accessed 20 October 2020].

Tor - Users. Available at: https://metrics.torproject.org/userstats-relay-country.html [accessed 22 September 2020].

Tor Blog (22 July 2018) How to do effective and impactful research. Available at: https://blog.torproject.org/how-do-effective-and-impactful-tor-research [accessed 8 January 2019].

Tor Metrics – China Users 2017-01-01 to 2018-01-01. Available at: https://metrics.torproject.org/userstats-relay-country.html?start=2017-01-01&end=2018-01-01&country=cn&events=off [accessed 1 February 2019].

Zerodium - Our exploitation acquisition program. Available at: https://zerodium.com/program.html [accessed 23 May 2020].

Unauthorised intelligence disclosures

CIA (21 December 2012) CIA advice for US government operatives infiltrating Schengen, WikiLeaks. Available at: https://WikiLeaks.org/cia-travel/infiltrating-schengen/WikiLeaks_CIA_Advice_for_Operatives_Infiltrating_Schengen.pdf [accessed 11 January 2018].

CIA (21 December 2014) CIA assessment on surviving secondary screening at airports while maintaining cover, WikiLeaks. Available at: https://WikiLeaks.org/cia-travel/secondary-screening/WikiLeaks_CIA_Assessment_on_Surviving_Secondary_Screening.pdf [accessed 11 January 2018].

CIA 'Engineering Development Group: DarkSeaSkies 1.0 User Requirements Documents, Wikileaks, 2009. Available at: https://wikileaks.org/vault7/darkmatter/document/DarkSeaSkies_1_0_URD/DarkSeaSkies_1_0_URD.pdf [accessed 24 May 2020], p, 1.

Dhami, M. K. Behavioural science support for JTRIG's (Join Threat Research and Intelligence Group) effects and online HUMINT operations, Statewatch, GCHQ. Available at: http://www.statewatch.org/news/2015/jun/behavioural-science-support-for-jtrigs-effects.pdf [accessed 1 January].

Snowden Archive - Contact mapping – tip-off to Diplomatic travel plans. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH6d2f.dir/doc.pdf [accessed 1 March 2018].

Snowden Archive – Welcome to the Snowden Digital Surveillance Archive. Available at: https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi [accessed 23 December 2020]

Snowden Archive (2 April 2015) NATO Civilian Intelligence Council - Cyber Panel National Input. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0fa7.dir/doc.pdf [accessed 31 October 2017]

Snowden Archive (2013) (S//REL to USA, FVEY) Subject: NSA intelligence relationship with Sweden, Snowden Archive. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH9385.dir/doc.pdf [accessed 10 January 2018].

Snowden Archive (4 October 2014) TOR stinks. Available at: https://edwardsnowden.com/docs/doc/tor-stinks-presentation.pdf [accessed 1 March 2018].

Snowden Archive (9 December 2013) Exploiting Terrorist Use of Games & Virtual Environments. Available at: https://cryptome.org/2013/12/nsa-gchq-spy-games.pdf [accessed 1 January 2018].

Stratfor (March 2010) Intelligence services, part 1: Espionage with Chinese characteristics, WikiLeaks. Available at: https://WikiLeaks.org/gifiles/attach/133/133464_INTEL_SERVICES_CHINA.pdf [accessed 11 January 2018].

Wikileaks – Vault 7: projects. Available at: https://wikileaks.org/vault7/#Scribbles [accessed 20 September 2020].

Wikileaks (24 August 2017) ExpressLane. Available at: https://wikileaks.org/vault7/#ExpressLane [accessed 04 August 2020].

Wikileaks (7 March 2017) Fine Dining (case officer toolset) concepts. Available at: https://wikileaks.org/ciav7p1/cms/page_20251099.html [accessed 21 August 2020].

Wikileaks (7 March 2017) Press release. Available at: https://wikileaks.org/ciav7p1/index.html [accessed 1 March 2018].

Wikileaks (7 March 2017) Vault 7: CIA hacking tools revealed. Available at: https://wikileaks.org/ciav7p1/? [accessed 21 August 2020].

Wikileaks (March 2017) Weeping angel (extending) engineering notes. Available at: https://wikileaks.org/ciav7p1/cms/page_12353643.html [accessed 1 March 2018].

News articles and miscellaneous

ABC News (7 March 2018) Sergei Skripal: the story behind the Russian double agent found poisoned on a bench in an English town. Available at: https://www.abc.net.au/news/2018-03-07/sergei-skripal-and-anna-chapman-what-we-know/9523970 [accessed 15 January 2021].

Aid, M. M. (2013) Inside the NSA's ultra-secret China hacking group, *Foreign Policy.* Available at: http://foreignpolicy.com/2013/06/10/inside-the-nsas-ultra-secret-china-hacking-group/ [accessed 10 January 2018].

Ars Technica (26 January 2018) Candid camera: Dutch hacked Russians hacking DNC, including security cameras. Available at: https://arstechnica.com/information-technology/2018/01/dutch-intelligence-hacked-video-cameras-in-office-of-russians-who-hacked-dnc/ [accessed 20 January 2020].

Austin, G. (11 July 2018) How good are China's cyber defences? *The Diplomat.* Available at: https://thediplomat.com/2018/07/how-good-are-chinas-cyber-defenses/ [accessed 23 November 2018].

Ball, J., Borger, J. & Greenwald, G. (6 September 2013) Revealed: how US and UK spy agencies defeat internet privacy and security, *The Guardian.* Available at: https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [accessed 10 January 2018].

Barrett, B. (7 March 2017) Don't let WikiLeaks scare you off of Signal and other encrypted chat apps, *Wired.* Available at: https://www.wired.com/2017/03/WikiLeaks-cia-hack-signal-encrypted-chat-apps/ [accessed 10 January 2018].

BBC News (1 November 2017) Explainer: What is Russia's new VPN law all about? Available at: http://www.bbc.co.uk/news/technology-41829726 [accessed 31 January 2018].

BBC News (10 December 2017) In your face: China's all-seeing state. Available at: http://www.bbc.co.uk/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state [accessed 11 January 2018].

BBC News (10 November 2014) How uninhabited islands soured China-Japan ties. Available at: http://www.bbc.co.uk/news/world-asia-pacific-11341139 [accessed 31 October 2017].

BBC News (11 February 2019) Russia considers 'unplugging' from Internet. Available at: https://www.bbc.co.uk/news/technology-47198426 [accessed 13 February 2019].

BBC News (11 November 2014) DarkHotel hackers targets company bosses in hotel rooms. Available at: http://www.bbc.co.uk/news/technology-30001424 [accessed 1 March 2018].

BBC News (14 March 2018) Russian soy: UK to expel 23 Russian diplomats. Available at: https://www.bbc.co.uk/news/uk-43402506 [accessed 20 March 2018].

BBC News (16 November 2018) Russia ‘sought access to UK visa issuing system’. Available at: https://www.bbc.co.uk/news/world-europe-46237634 [accessed 5 November 2020).

BBC News (19 January 2012) UK spied on Russians with fake rock. Available at: https://www.bbc.co.uk/news/world-europe-16614209 [accessed 18 January 2021].

BBC News (19 January 2018) Mattis: US national security focus no longer terrorism. Available at: https://www.bbc.co.uk/news/world-us-canada-42752298 [accessed 3 February 2018].

BBC News (2 October 2010) Iran arrests ‘nuclear spies’ accused of cyber attacks. Available at: https://www.bbc.co.uk/news/world-middle-east-11459468 [accessed 1 March 2017].

BBC News (21 January 2016) Alexander Litvinenko: profile of murdered Russian spy. Available at: http://www.bbc.co.uk/news/uk-19647226 [accessed 31 November 2017].

BBC News (21 September 2016) MI6 set to recruit 1,000 extra staff. Available at: http://www.bbc.co.uk/news/uk-37434131 [accessed 10 January 2018].

BBC News (22 July 2019) Russian intelligence ‘targets Tor anonymous browser’. Available at: https://www.bbc.co.uk/news/technology-49071225 [accessed 20 September 2020].

BBC News (22 March 2010) Biofuel bus driver fined over sat phone use in India. Available at: http://news.bbc.co.uk/1/hi/england/london/8579614.stm [accessed 20 February 2018].

BBC News (23 April 2018) Russia Telegram ban hits Google and Amazon services. Available at: https://www.bbc.co.uk/news/technology-43865538 [accessed 20 November 2018].

BBC News (23 September 2015) Does China’s government hack US companies to steal secrets? Available at: http://www.bbc.co.uk/news/technology-34324252 [accessed 31 October 2017].

BBC News (24 December 2019) Russia ‘successfully tests’ its unplugged internet. Available at: https://www.bbc.co.uk/news/technology-50902496 [accessed 20 March 2020].

BBC News (24 July 2017) China set to launch an ‘unhackable’ internet communication. Available at: http://www.bbc.co.uk/news/world-asia-40565722 [accessed 10 January 2018].

BBC News (24 July 2020) US consulate: China orders US consulate closure in tit-for-tat move. Available at: https://www.bbc.co.uk/news/world-asia-china-53522640 [accessed 13 September 2020].

BBC News (25 April 2017) Russian hackers ‘target’ presidential candidate Macron. Available at: https://www.bbc.co.uk/news/technology-39705062 [accessed 23 January 2020].

BBC News (26 July 2020) How a Chinese agent used LinkedIn to hunt for targets. Available at: https://www.bbc.co.uk/news/world-asia-53544505 [accessed 12 August 2020].

BBC News (27 April 2017) How a cyber attack transformed Estonia. Available at: http://www.bbc.co.uk/news/39655415 [accessed 31 November 2017].

BBC News (27 March 2017) WhatsApp's privacy protections questioned after terror attack. Available at: https://www.bbc.co.uk/news/technology-39405178 [accessed 12 May 2020].

BBC News (27 May 2019) Russian data theft: shady world where all is for sale. Available at: https://www.bbc.co.uk/news/world-europe-48348307 [accessed 12 May 2020].

BBC News (28 February 2015) Sir John Sawers, ex-MI6 chief, warns of Russia 'danger'. Available at: http://www.bbc.co.uk/news/uk-31669195 [accessed 31 November 2017].

BBC News (28 July 2014) Russia offers $110, 000 to crack Tor anonymous network. Available at: https://www.bbc.co.uk/news/technology-28526021 [accessed 20 June 2017].

BBC News (28 March 2010) Dubai's starring role in Israeli-linked murder plot. Available at: http://news.bbc.co.uk/1/hi/world/middle_east/8588873.stm [accessed 21 August 2020].

BBC News (29 June 2010) Long history of deep-cover 'illegals'. Available at: http://www.bbc.co.uk/news/10452384 [accessed 31 November 2017].

BBC News (3 February 2015) Facial recognition technology: How well does it work? Available at: http://www.bbc.co.uk/news/technology-31112604 [accessed 11 January 2018].

BBC News (5 October 2015) Edward Snowden interview: 'smartphones can be taken over'. Available at: http://www.bbc.co.uk/news/uk-34444233 [accessed 1 January 2018].

BBC News (5 October 2016) NATO jets scrambled as Russian bombers fly south. Available at: http://www.bbc.co.uk/news/world-europe-37562499 [accessed 31 October 2017].

BBC News (5 October 2017) Russian soldiers face ban on selfies and blog posts. Available at: http://www.bbc.co.uk/news/world-europe-41510592?ocid=socialflow_twitter [accessed 1 January 2018].

BBC News (7 October 2016) US accuses Russia of cyber attacks. Available at: http://www.bbc.co.uk/news/election-us-2016-37592684 [accessed 31 November 2017].

BBC News (8 October 2018) Russian spy poisoning: what we know so far. Available at: https://www.bbc.co.uk/news/uk-43315636 [accessed 20 October 2018].

Bearman, J., Hanuka, T., Davis, J. & Leekart, S. (May 2015) The rise and fall of Silk Road: how a 29-year-old idealist built a global drug bazaar and became a murderous kingpin, *Wired*. Available at: https://www.wired.com/2015/04/silk-road-1/ [accessed 14 July 2017].

Bennett, B. & Hennigan, W. J. (31 August 2015) China and Russia are using hacked data to target U.S. spies, officials say, *Los Angeles Times.* Available at: http://www.latimes.com/nation/la-na-cyber-spy-20150831-story.html [accessed 11 January 2018].

Blizzard reaches 100M lifetime World of Warcraft accounts (28 January 2014) Polygon. Available at: https://www.polygon.com/2014/1/28/5354856/world-of-warcraft-100m-accounts-lifetime [accessed 20 March 2020].

Bloomberg (1 August 2016) CIA cyber official sees data flood as both godsend and danger. Available at: https://www.bloomberg.com/news/articles/2016-08-01/cia-cyber-official-sees-data-flood-as-both-godsend-and-danger [accessed 11 January 2018].

Bloomberg (12 February 2012) AP impact: USAID contractor work in Cuba detailed. Available at: http://www.businessweek.com/ap/financialnews/D9SSHGPG2.htm [accessed 12 March 2018].

Bloomberg (22 September 2015) Russia's plan to crack Tor crumbles. Available at: https://www.bloomberg.com/news/articles/2015-09-22/russia-s-plan-to-crack-tor-crumbles [accessed 1 March 2018].

Bloomberg (25 September 2017) Natalya Kaspersky's snoop=proof phone helps Putin thwart spies. Available at: https://www.bloomberg.com/news/articles/2017-09-25/natalya-kaspersky-s-snoop-proof-phone-helps-putin-thwart-spies [accessed 1 March 2018].

Bowcott, O & Norton-Taylor, R. (21 April 2016) UK spy agencies have collected bulk personal data since 1990s, files show, *The Guardian.* Available at: https://www.theguardian.com/world/2016/apr/21/uk-spy-agencies-collected-bulk-personal-data-since-1990s [accessed 1 March 2018].

Bradshaw, T. (21 November 2017) Apple drops hundreds of VPN apps at Beijing's request, *Financial Times.* Available at: https://www.ft.com/content/ad42e536-cf36-11e7-b781-794ce08b24dc [accessed 25 November 2017].

Bradsher, K. (25 September 2017) China blocks WhatsApp, broadening online censorship, *The New York Times.* Available at: https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html [accessed 3 November 2017].

Brannen, K. (6 April 2015) To catch a spy, *Foreign Policy.* Available at: http://foreignpolicy.com/2015/04/06/to-catch-a-spy-biometrics-cia-border-security/ [accessed 12 January 2018].

Bridge, M. (19 June 2019) Russians created AI redhead on LinkedIn to steal military secrets, *The Times.* Available at: https://www.thetimes.co.uk/article/russians-created-ai-redhead-on-linkedin-to-steal-military-secrets-k2d20lc2z [accessed 1 December 2020].

Brookes, A. (4 November 2014) Is China swarming with foreign spies?, *Foreign Policy*. Available at: http://foreignpolicy.com/2014/11/04/is-china-swarming-with-foreign-spies/ [accessed 11 January 2018].

Burgess, M. (28 April 2018) This is why Russia's attempts to block Telegram have failed, *Wired*. Available at: https://www.wired.co.uk/article/telegram-in-russia-blocked-web-app-ban-facebook-twitter-google [accessed 20 November 2018].

Burgess, M. (7 May 2017) Wikileaks drops 'Grasshopper' documents, part four of its CIA Vault 7 files, *Wired*. Available at: https://www.wired.co.uk/article/cia-files-wikileaks-vault-7 [accessed 1 March 2018].

Burgess, M. (9 May 2017) WhatsApp now encrypts iCloud back-ups of your conversations, *Wired*. Available at: http://www.wired.co.uk/article/WhatsApp-encryption-end-to-end-turned-on [accessed 1 March 2018].

Business Insider (1 September 2015) Russia and China could be 'making it impossible for the US to hide' its intelligence activities. Available at: http://uk.businessinsider.com/russia-china-us-intelligence-database-2015-8 [accessed 11 January 2018].

Business Insider (13 December 2013) NSA: Snowden stole 1.7 million classified documents and still has access to most of them. Available at: http://www.businessinsider.com/how-many-docs-did-snowden-take-2013-12?IR=T [accessed March 1 2018]

Business Insider (13 February 2018) The NSA sent coded messages to a shadow Russian on its official Twitter account. Available at: https://www.businessinsider.com/nsa-sent-coded-messages-to-russian-using-its-official-twitter-account-2018-2?r=US&IR=T [accessed 14 March 2019].

Business Insider (20 September 2016) Russia busts pair 'trying to sell CIA fake secrets'. Available at: https://www.businessinsider.com/afp-russia-busts-pair-trying-to-sell-cia-fake-secrets-2016-9?r=US&IR=T [accessed 15 September 2020].

Business Insider (3 December 2017) British security services are vastly outgunned by the Russian counterintelligence threat. Available at: http://uk.businessinsider.com/british-security-services-vs-russian-counterintelligence-threat-2017-12 [accessed 10 January 2018].

Business Insider (8 March 2017) Wikileaks' dump of CIA hacking tools is 'devastating' for the agency – but there may be an upside. Available at: https://www.businessinsider.com/wikileaks-dump-of-cia-hacking-tools-2017-3?r=US&IR=T [accessed 24 August 2020].

Callick, R. (9 December 2016) China's all-seeing spy grid takes surveillance to new level, *The Australian.* Available at: http://www.theaustralian.com.au/news/inquirer/chinas-allseeing-spy-grid-takes-surveillance-to-new-level/news-story/7dfdf3fef86da6b8203c6acba3840539 [accessed 11 January 2018].

CBS News (11 September 2016) 9/11: Nunes, Salvanto, Brennan. Available at: https://www.cbsnews.com/videos/911-nunes-salvanto-brennan/ [accessed 31 November 2017].

China Law Translate (11 July 2016) 2016 cybersecurity law. Available at: http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en [accessed 21 January 2018].

Chitra, R. (26 August 2017) WikiLeaks hints at CIA access to Adhaar data, officials deny it, *The Times of India.* Available at: https://timesofindia.indiatimes.com/india/WikiLeaks-hints-at-cia-access-to-aadhaar-data-officials-deny-it/articleshow/60228184.cms [accessed 11 January 2018].

Clayton Utz (7 December 2017) Comply or be prepared to pay: China's new cybersecurity law. Available at: https://www.claytonutz.com/knowledge/2017/december/comply-or-be-prepared-to-pay-chinas-new-cybersecurity-law [accessed 1 June 2018].

CNBC (8 January 2016) There's a hack for that: Fitbit user accounts attacked. Available at: https://www.cnbc.com/2016/01/08/theres-a-hack-for-that-fitbit-user-accounts-attacked.html [accessed 12 May 2020].

CNN (14 June 2017) 146,000 cameras monitor Moscow streets. And the government is just getting started. Available at: http://money.cnn.com/2017/06/14/technology/culture/moscow-cameras/index.html [accessed 11 January 2018].

CNN (16 March 2018) Trump expelling 60 Russian diplomats in wake of UK nerve agent attack. Available at: https://edition.cnn.com/2018/03/26/politics/us-expel-russian-diplomats/index.html [accessed 3 April 2018].

CNN (17 October 2017) Exclusive: Putin's 'chef,' the man behind the troll factory. Available at http://edition.cnn.com/2017/10/17/politics/russian-oligarch-putin-chef-troll-factory/index.html [accessed 10 January 2018].

CNN (23 May 2017) Transcripts. Available at: http://transcripts.cnn.com/TRANSCRIPTS/1705/23/cnr.03.html [accessed 24 October 2017].

CNN (24 August 2017) FBI arrests Chinese national connected to malware used in OPM data breach. Available at: http://edition.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html [accessed 2 November 2017].

CNN (25 October 2017) Exclusive: Mueller's team met with Russia dossier author. Available at: https://edition.cnn.com/2017/10/05/politics/special-counsel-russia-dossier-christopher-steele/index.html [accessed 26 Octomber 2017].

CNN (27 June 2017) How one typo helped let Russian hackers in. Available at: http://edition.cnn.com/2017/06/27/politics/russia-dnc-hacking-csr/index.html [accessed 31 November 2017]

CNN (27 September 2017) Top US general: China will be ‘greatest threat’ to US by 2025. Available at: http://edition.cnn.com/2017/09/26/politics/dunford-us-china-greatest-threat/index.html [October 31 2017]

CNN (29 March 2018) Russia expels US diplomats and shuts consulate in tit-for-tat move. Available at: https://edition.cnn.com/2018/03/29/europe/russia-expels-us-diplomats-intl/index.html [accessed 21 November 2019].

CNN (30 September 2015) U. S. pulls spies from China after hack. Available at: http://money.cnn.com/2015/09/30/technology/china-opm-hack-us-spies/index.html [accessed 10 January 2018].

CNN (8 March 2017) Analyst says Wikileaks dump ‘devastating’ for CIA. Available at: https://edition.cnn.com/2017/03/08/politics/philip-mudd-cia-wikileaks/index.html [accessed March 1 2018].

Committee to Protect Journalists (24 February 2012) Caveat utilitor: Satellite phones can always be tracked. Available at: https://cpj.org/2012/02/caveat-utilitor-satellite-phones-can-always-be-tra/ [accessed 23 July 2020].

Computer World (23 March 2017) Snowden’s ex-boss offers advice on stopping insider threats. Available at: https://www.computerworld.com/article/3184411/security/snowdens-ex-boss-offers-advice-on-stopping-insider-threats.html [accessed March 1 2018].

Consumer Reports (7 February 2018) Samsung and Roku smart TVs vulnerable to hacking, consumer reports finds. Available at: https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/ [accessed 23 March 2020].

Corera, G. (7 April 2016) The spies of tomorrow will need to love data, *Wired*. Available at: http://www.wired.co.uk/article/spies-data-mi6-cia-gordon-corera [accessed 11 January 2018].

Couceiro, C. (March 2017) How the CIA forgot the art of spying, *Politico.* Available at: https://www.politico.com/magazine/story/2017/03/cia-art-spying-espionage-spies-military-terrorism-214875 [accessed 20 January 2018].

CRN (7 August 2015) Pentagon data breach shows growing sophistication of phishing attacks. Available at: https://www.crn.com/news/security/300077701/pentagon-data-breach-shows-growing-sophistication-of-phishing-attacks.htm [accessed 23 May 2020].

CSIS - Transcripts – The national security division at 10. Available at: https://www.csis.org/transcripts-national-security-division-10 [accessed 1 March 2018].

CSO from IDG (17 April 2018) The 18 biggest data breaches of the 21st century. Available at: https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html [accessed 23 December 2018].

CSO Online (14 July 2014) 4 reasons why executives are the easiest social engineering targets. Available at: https://www.csoonline.com/article/2125311/social-engineering/4-

reasons-why-executives-are-the-easiest-social-engineering-targets.html [accessed 1 March 2018].

Cuthbertson, A. (11 December 2017) China is spying on the west using LinkedIn, intelligence agency claims, *Newsweek.* Available at: http://www.newsweek.com/china-spying-west-using-linkedin-743788 [accessed 1 January 2018].

Daily Beast (5 May 2017) Is there a Russian mole inside the NSA? The CIA? Both? Available at: https://www.thedailybeast.com/is-there-a-russian-mole-inside-the-nsa-the-cia-or-both [accessed March 1 2018].

Datacenter Dynamics (14 September 2015) Russian data law: Apple complies, Google and Facebook delay. Available at: http://www.datacenterdynamics.com/content-tracks/design-build/russian-data-law-apple-complies-google-and-facebook-delay/94785.fullarticle [accessed 31 January 2018].

Defense One (1 October 2015) Meet the man reinventing CIA for the big data era. Available at: http://www.defenseone.com/technology/2015/10/meet-man-reinventing-cia-big-data-era/122453/ [accessed 11 January 2018].

Defense One (6 March 2015) CIA restructuring adds new cyber focus. Available at: http://www.defenseone.com/technology/2015/03/cia-restructuring-adds-new-cyber-focus/106953/ [accessed 11 January 2018]

Der Spiegel (May 3 2018) cyber-espionage hits Berlin: the breach from the East. Available at: http://www.spiegel.de/international/germany/cyber-espionage-likely-from-russia-targets-german-government-a-1196520.html [accessed 5 March 2018]

Digiday (18 November 2014) Seriously dark traffic: 500 mil. People globally hide their IP addresses. Available at: https://digiday.com/uk/vpn-hide-ip-address-distort-analytics/ [accessed 21 March 2020].

Dorfman, Z. (15 August 2018) Botched CIA communications system helped blow cover of Chinese agents, *Foreign Policy.* Available at: https://foreignpolicy.com/2018/08/15/botched-cia-communications-system-helped-blow-cover-chinese-agents-intelligence/ [accessed 1 November 2018].

Dou, E. & Osawa, J. (20 November 2015) China to build its own secure smartphones, *The Australian.* Available at: https://www.theaustralian.com.au/business/business-spectator/china-to-build-its-own-secure-smartphones/news-story/2ca15fd9c3683ae36fc8a1bb5da7c7c8 [accessed 1 March 2018].

Drury, I. & Williams, D. (10 August 2015) Foreign spies on LinkedIn trying to recruit civil servants by 'befriending' them before stealing British secrets, *Daily Mail*. Available at: https://www.dailymail.co.uk/news/article-3191733/Foreign-spies-LinkedIn-trying-recruit-civil-servants-befriending-stealing-British-secrets.html [accessed 12 March 2018].

Economy, E. C. (29 Jun 2018) The Great Firewall of China: Xi Jinping's internet shutdown, *The Guardian.* Available at https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown [accessed 12 June 2020].

Elder, M. (11 July 2013) Russian guard service reverts to typewriters after NSA leaks, *The Guardian.* Available at: https://www.theguardian.com/world/2013/jul/11/russia-reverts-paper-nsa-leaks [accessed 13 September 2020].

Evans, M. (5 March 2018) Sergei Skripal: the 'spy with the Louis Vuitton bag' allegedly poisoned during retirement in Salisbury, *The Telegraph.* Available at: https://www.telegraph.co.uk/news/2018/03/05/sergei-skripalthe-spy-louis-vuitton-bag-allegedly-poisoned-quiet/ [accessed 13 October 2020].

ExpressVPN - What is a VPN for? Available at: https://www.expressvpn.com/internet-privacy/guides/who-uses-vpn/ [accessed 20 July 2020].

Farmer, B. (31 August 2015) British spies trawl Ashley Madison leak for intelligence, *The Telegraph.* Available at: http://www.telegraph.co.uk/news/uknews/defence/11830594/British-spies-trawl-Ashley-Madison-leak-for-intelligence.html [accessed 1 March 2018].

FCW (1 October 2015) Inside the CIA's new digital directorate. Available at: https://fcw.com/Articles/2015/10/01/CIA-digital-directorate.aspx?Page=1 [accessed 11 January 2018].

Financial Times (11 January 2017) The changing face of Russian cyber espionage. Available at: https://www.ft.com/content/ea9f93fc-b721-4783-aa7a-d88b3e4e2042 [accessed 31 November 2017].

Fish, I. S. (24 December 2015) Why can't ex-Chinese leaders travel abroad, *Foreign Policy.* Available at: https://foreignpolicy.com/2015/12/24/why-are-former-chinese-leaders-prevented-from-traveling-overseas-xi-jinping/ [accessed 11 January 2018].

Gao, H. (2 February 2015) China sharpens its censorship blade, *The New York Times.* Available at: https://www.nytimes.com/2015/02/03/opinion/china-sharpens-its-censorship-blade.html?_r=0 [accessed 10 January 2018].

Ge, C. (19 April 2016) PLA on call: China's military orders anti-spy software for soldiers' smartphones, *South China Morning Post.* Available at: https://www.scmp.com/news/china/diplomacy-defence/article/1937085/pla-call-chinas-military-orders-anti-spy-software [accessed 1 January 2018].

Global Times (28 August 2014) Peeking in China: spying targets and tactics. Available at: http://www.globaltimes.cn/content/878779.shtml [accessed 20 March 2016].

Greenberg, A. (11 January 2017) How spy agency vets read that bombshell Trump report: with caution, *Wired*. Available at: https://www.wired.com/2017/01/spy-agency-vets-read-bombshell-trump-report-caution/ [accessed 31 November 2017].

Greenberg, A. (16 December 2013) An NSA coworker remembers the real Edward Snowden: 'a genius among geniuses', *Forbes*. Available at: https://www.forbes.com/sites/andygreenberg/2013/12/16/an-nsa-coworker-remembers-the-real-edward-snowden-a-genius-among-geniuses/#342cb66e784e [accessed March 1 2018].

Greenberg, A. (18 November 2015) Here's a spy firm's price list for secret hacker techniques, *Wired*. Available at: https://www.wired.com/2015/11/heres-a-spy-firms-price-list-for-secret-hacker-techniques/ [accessed 1 January 2018].

Greenberg, A. (20 June 2017) How an entire nation became Russia's test lab for cyberwar, *Wired*. Available at: https://www.wired.com/story/russian-hackers-attack-ukraine/ [accessed 31 November 2017].

Greenberg, A. (23 March 2017) Wikileaks reveals how the CIA can hack a mac's hidden code, *Wired*. Available at: https://www.wired.com/2017/03/wikileaks-shows-cia-can-hack-macs-hidden-code/ [accessed 1 March 2018].

Greenberg, A. (30 December 2014) Over 80 percent of dark-web visits relate to paedophilia, study finds, *Wired*. Available at: https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/ [accessed 23 July 2020].

Greenberg, A. (31 October 2017) China tests the limits of its US hacking truce, *Wired*. Available at: https://www.wired.com/story/china-tests-limits-of-us-hacking-truce/ [accessed 2 October 2017].

Greenberg, A. (4 October 2016) You can all finally encrypt Facebook messenger, so do it, *Wired*. Available at: https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/ [accessed 11 January 2018].

Greenberg, A. (7 March 2017) How the CIA can hack your phone, PC, and TV (says Wikileaks), *Wired*. Available at: https://www.wired.com/2017/03/cia-can-hack-phone-pc-tv-says-wikileaks/ [accessed 1 December 2017].

Greenwald, G. & MacAskill, E. (6 June 2013) NSA Prism program taps in to user data of Apple, Google and others, *The Guardian.* Available at: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Network%20front:network-front%20main-2%20Special%20trail:Network%20front%20-%20special%20trail:Position1 [accessed 19 March 2019].

Haas, B. (11 July 2017) China moves to block internet VPNs from 2018, *The Guardian.* Available at: https://www.theguardian.com/world/2017/jul/11/china-moves-to-block-internet-vpns-from-2018 [accessed 11 January 2018].

Haas, B. (22 December 2017) Man in China sentences to five years' jail for running VPN, *The Guardian.* Available at: https://www.theguardian.com/world/2017/dec/22/man-in-china-sentenced-to-five-years-jail-for-running-vpn [accessed 20 January 2018].

Haas, B. (7 August 2018) China bans Winnie the Pooh film after comparisons to President Xi, *The Guardian.* Available at: https://www.theguardian.com/world/2018/aug/07/china-bans-winnie-the-pooh-film-to-stop-comparisons-to-president-xi [accessed 13 June 2020].

HackersOnBoard (19 November 2013) BlackHat 2013 – Combating the insider threat at the FBI: Real-world lessons learned. Available at: https://www.youtube.com/watch?v=38M8ta13K0Q [accessed 1 March 2018]

Harding, L. (29 December 2018) ‘Will they forgive me? No’: ex-Soviet spy Viktor Suvorov speaks out, *The Guardian.* Available at: https://www.theguardian.com/world/2018/dec/29/ex-soviet-spy-viktor-suvorov [accessed 29 December 2018].

Harding, L. (3 February 2018) Why Carter Page was worth watching, *Politico.* Available at: https://www.politico.com/magazine/story/2018/02/03/carter-page-nunes-memo-216934 [accessed 24 February 2018].

Harper, T. (14 June 2015) British spies betrayed to Russians and Chinese, *The Times.* Available at: https://www.thetimes.co.uk/article/british-spies-betrayed-to-russians-and-chinese-xxj7zx5n83d [accessed 22 November 2016].

Hearst, D. (29 June 2010) ‘Russian spies’ bungle was epic, *The Guardian.* Available at: https://www.theguardian.com/commentisfree/2010/jun/29/russian-spies-bungle-epic [accessed 31 November 2017].

Higgins, A. & Kramer, A. E. (11 January 2017) Russia’s sexual blackmail didn’t die with the Soviets, *The New York Times.* Available at: https://www.nytimes.com/2017/01/11/world/europe/donald-trump-russia.html [accessed 10 January 2018].

Hovel, R. (16 January 2014) Nuclear researcher fired for connecting USB flash drive to work computer, *Haaretz*. Available at: https://www.haaretz.com/.premium-nuclear-researcher-fired-over-usb-1.5312577 [accessed 1 March 2018].

Huffington Post (12 June 2018) At the CIA, a fix to communications system that left trail of dead agents remains elusive. Available at: https://www.huffingtonpost.com/entry/at-the-cia-a-fix-to-communications-system-that-left-trail-of-dead-agents-remains-elusive_us_5c094117e4b069028dc7696a [accessed 15 March 2019].

Huffington Post (3 June 2019) Nearly all U.S. visa applicants now required to submit 5-year social media history. Available at: https://www.huffingtonpost.co.uk/entry/visa-social-media-state-department_n_5cf4898ce4b0e8085e3bfde1?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAImALRHTwaQyk9Lu3BCqYlCdJjsHnXXur6Gu-UCvjyknbwpH-hjDYnM_5gsx3zelhVO05YVF_migMklpe3CyyQvPSHXaituIb3iLew56P8YH3_0i40dTZkT3LVrkSRhauyRuNwT_MGWfP4c8tkQaeWpPkDnKyAr0a1ANiCQdfIqo [accessed 10 July 2019].

Huffington Post (6 December 2016) Once a defender of Internet freedom, Putin is now bringing China’s Great Firewall to Russia. Available at: https://www.huffingtonpost.com/andrei-soldatov/putin-china-internet-firewall-russia_b_9821190.html [accessed 31 January].

Huffington Post (9 October 2019) CIA reportedly had asset so close to Putin that spy could photograph secret documents. Available at: https://www.huffingtonpost.co.uk/entry/cia-russia-informant-putin-extracted_n_5d76f3b5e4b0fde50c2bbc9b?ri18n=true&guce_referrer=aHR0cHM6Ly93

d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAEL88NGqHuZX2Rf4j8ccflWs0nh5OsAvuEKSmbA1o63umH5m0gjbbZtAcy1D3GlWf6uUXyG8WijoxysZdPU8uBxFt2MPMRvHsEXKYjs-38YREnLmBken4G7MGxBTSjPmTToih8hHmOOV_zUDX4Tia5WTdyg9qin33CPTSujs4cqx&guccounter=2 [accessed 20 September 2020].

Huggler, J. (July 2014) Germany demands full explanation from US on arrested spy, *The Telegraph.* Available at: https://www.telegraph.co.uk/news/worldnews/europe/germany/10949568/Germany-demands-full-explanation-from-US-on-arrested-spy.html [accessed 23 March 2020].

IBM Knowledge Center – National Security Agency (NSA) Suit B cryptography. Available at: https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy11025_.htm [accessed 1 July 2018].

Independent (22 October 2016) Russian ambassador to UK claims embassy is 'shrinking' because government is delaying staff visas. Available at: http://www.independent.co.uk/news/uk/home-news/russian-ambassador-embassy-shrinking-delay-visas-staff-alexander-yakovenko-foreign-office-a7375171.html [accessed 10 January 2018].

Independent (9 February 2017) China to take fingerprints of all foreign travellers entering country. Available at http://www.independent.co.uk/news/world/asia/china-fingerprints-tourist-visits-scanning-customs-a7571871.html [accessed 11 January 2017].

itNews (4 March 2014) Israeli spies banned from biometric ID cards, passports. Available at: https://www.itnews.com.au/news/israeli-spies-banned-from-biometric-id-cards-passports-373849 [accessed 11 January 2018].

Jones, S. (28 September 2016) The spy who liked me: Britain's changing secret service. *Financial Times.* Available at: https://www.ft.com/content/b239dc22-855c-11e6-a29c-6e7d9515ad15 [accessed 1 March 2018].

Jones, S. (7 August 2014) Ukraine PM's office hit by cyber attack linked to Russia, *Financial Times.* Available at: https://www.ft.com/content/2352681e-1e55-11e4-9513-00144feabdc0 [accessed 31 November 2017].

Judah, B. (19 October 2014) Putin's coup: How the Russian leader used the Ukraine crisis to consolidate his dictatorship, *Politico*. Available at: https://www.politico.com/magazine/story/2014/10/vladimir-putins-coup-112025_full.html#.WJo84H9yXE9 [accessed 1 March 2018].

Kaspersky Daily (3 May 2016) Hackers broadcast live footage from hacked webcams on YouTube and trolls are loving it. Available at: https://www.kaspersky.co.uk/blog/2ch-webcam-hack/7120/ [accessed 25 May 2020].

Katwala, A. (17 May 2018) We're calling it: PGP is dead, *Wired*. Available at: https://www.wired.co.uk/article/efail-pgp-vulnerability-outlook-thunderbird-smime [accessed 20 March 2020].

Koerner, B. I. (23 October 2016) Inside the cyberattack that shocked the US government, *Wired*. Available at: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ [accessed 1 March 2018].

KrebsonSecurity (8 March 2017) Wikileaks dumps docs on CIA's hacking tools, Krebs on Security, 2017. Available at: https://krebsonsecurity.com/tag/vault-7/ [accessed 25 June 2020].

Kupfer, M. & Bodner, M. (19 January 2017) Spy games: how the spectre of surveillance impacts Moscow's foreigners, *The Moscow Times*. Available at: https://themoscowtimes.com/articles/spy-games-how-the-spectre-of-surveillance-impacts-the-lives-of-moscows-foreigners-56865 [accessed 13 February 2018].

Landler, M. & Chan, S. (25 October 2010) Taking harder stance toward China, Obama lines up allies, *The New York Times.* Available at: http://www.nytimes.com/2010/10/26/world/asia/26china.html [accessed 31 October 2017].

Lewis, J. (10 March 2012) How spies used Facebook to steal NATO chiefs' details, *The Telegraph.* Available at: https://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefs-details.html [accessed 16 March 2019].

Li, E. (6 July 2017) For many Chinese Internet users, it's time to get a new VPN, *South China Morning Post*. Available at: https://www.scmp.com/news/china/policies-politics/article/2101435/many-chinese-internet-users-its-time-get-new-vpn [accessed 23 July 2020].

LinkedIn (10 August 2015) LinkedIn used by Chinese & Russian spies to recruit Brits & steal secrets. Available at: https://www.linkedin.com/pulse/linkedin-used-chinese-russian-spies-recruit-brits-steal-lee-blasdale [accessed 1 January 2018].

Lior, I. (3 March 2014) Shin Bet, Mossad bar employees from signing up for biometric database, *Haaretz*. Available at: http://www.haaretz.com/israel-news/.premium-1.577516 [accessed 11 January 2018].

Lucas, E. (1 December 2018) MI6 lays bare the growing Russian threat, *The Times*. Available at: https://www.thetimes.co.uk/edition/comment/mi6-lays-bare-the-growing-russian-threat-sg6vcvl22 [accessed 10 January 2018].

Luhn, A. (26 June 2016) Russia passes 'Big Brother' anti-terror laws, *The Guardian.* Available at: https://www.theguardian.com/world/2016/jun/26/russia-passes-big-brother-anti-terror-laws [accessed 21 January 2021].

MacAskill, E. (24 April 2014) Putin calls Internet a 'CIA project' renewing fears of web breakup, *The Guardian.* Available at: https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia [accessed 20 August 2016].

Mackinnon, A. (28 January 2019) Hackers turn the tables on Russia, *Foreign Policy.* Available at: https://foreignpolicy.com/2019/01/28/hackers-turn-the-tables-on-russia-hacking-leaking-cyber-documents-wikileaks/ [accessed 19 March 2019].

Manson, K., Shubber, K. & Murphy, H. (30 July 2020) LinkedIn spy scandal shines spotlight on China's online espionage, *Financial Times*. Available at: https://www.ft.com/content/0a0e62a9-65ba-494c-a7bb-86f5f66d627f [accessed 1 December 2020].

Mazetti, M. & Elliott, J. (10 December 2013) Spies infiltrate a fantasy realm of online games, *The New York Times.* Available at: http://www.nytimes.com/2013/12/10/world/spies-dragnet-reaches-a-playing-field-of-elves-and-trolls.html?mtrref=onlinelibrary.wiley.com&gwh=EE5694212E9FCD4467863E62E311F74E&gwt=pay [accessed 1 January 2018].

Mazetti, M. & Goldman, A. (30 December 2016) 'The game will go on' as U.S. expels Russian diplomats, *The New York Times.* Available at: https://www.nytimes.com/2016/12/30/us/politics/obama-russian-spies.html [accessed 10 January 2018].

Mazetti, M. (24 May 2013) New terror strategy shifts C.I.A, *The New York Times.* Available at: http://www.nytimes.com/2013/05/24/us/politics/plan-would-orient-cia-back-toward-spying.html [accessed 10 January 2018].

Mazetti, M., Goldman, A., Schmidt, M. S. & Apuzzo, M. (20 May 2017) Killing C.I.A. informants, China crippled U.S. spying operations, *The New York Times.* Available at: https://www.nytimes.com/2017/05/20/world/asia/china-cia-spies-espionage.html [accessed 1 January 2018].

McGreal, C. (9 March 2016) America's former CIA chief: 'If we don't handle China well, it will be catastrophic', *The Guardian.* Available from https://www.theguardian.com/us-news/2016/mar/09/america-cia-nsa-chief-general-michael-hayden-china-catastrophic-for-world [accessed 12 October 2020].

Meduza (10 April 2019) Russia's censorship agency has threatened to block OpenVPN. At worst, that move could interfere with systems from banking to cell service. Available at: https://meduza.io/en/feature/2019/04/10/russia-s-censorship-agency-has-threatened-to-block-openvpn-at-worst-that-move-could-intefere-with-systems-from-banking-to-cell-service [accessed 18 January 2020].

Meduza (19 July 2017) Moscow's cyber-defense: how the Russian government plans to protect the country from the coming cyberwar. Available at: https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense [accessed 15 March 2017].

Meduza (23 May 2018) Russia finds a new Tor criminal: How Dmitry Bogatov went from suspect to witness. Available at: https://meduza.io/en/feature/2018/05/23/russia-finds-a-new-tor-criminal [accessed 27 May 2018].

Meduza (24 June 2015) Russia's state Duma just approved some of the most repressive laws in post-Soviet history. Available at: https://meduza.io/en/feature/2016/06/24/russia-s-state-duma-just-approved-some-of-the-most-repressive-laws-in-post-soviet-history [accessed 24 January 2018].

Meduza (31 July 2019) 'I'd be willing to work against this government with Satan himself' We talked to a suburban Russian policeman who spied for the CIA, fought in eastern Ukraine, and got sentence to 13 years for treason. Available at: https://meduza.io/en/feature/2019/07/31/i-d-be-willing-to-work-against-this-government-with-satan-himself [accessed 15 September 2020].

Meduza (6 August 2019) How and why the Russian military puts soldiers in jail for using smartphones and social media. Available at: https://meduza.io/en/feature/2019/08/06/how-and-why-the-russian-military-puts-soldiers-in-jail-for-using-smartphones-and-social-media [accessed 21 March 2020].

Meduza (9 September 2015) The Russian government hired people to hack to the Tor browser, but they failed and now they're quitting. Available at: https://meduza.io/en/news/2015/09/09/the-russian-government-hired-people-hack-the-tor-browser-but-they-failed-and-now-they-re-quitting [accessed 1 March 2018].

Meyer, D. (29 January 2016) Here's how much Google paid out to security researchers last year, *Fortune.* Available at: https://fortune.com/2016/01/29/heres-how-much-google-paid-out-to-security-researchers-last-year/ [accessed 12 May 2020].

Miller, G. (14 September 2016) As Russia reasserts itself, U.S. intelligence agencies focus anew on the Kremlin, *The Washington Post.* Available at: https://www.washingtonpost.com/world/national-security/as-russia-reasserts-itself-us-intelligence-agencies-focus-anew-on-the-kremlin/2016/09/14/cc212c62-78f0-11e6-ac8e-cf8e0dd91dc7_story.html?postshare=3714739568243 84&tid=ss_tw-bottom&utm_term=.d8941ad4f02e#comments [accessed 31 November 2017].

Miller, G., Nakashima, E. & Entous, A. (23 June 2017) Obama's secret struggle to punish Russia for Putin's election assault, *The Washington Post.* Available at: https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.73bfdde12b13 [accessed 10 January 2018].

MIT News (26 February 2020) Protecting sensitive metadata so it can't be used for surveillance. Available at: https://news.mit.edu/2020/protecting-sensitive-metadata-from-surveillance-0226 [accessed 15 January 2021].

MIT Technology Review (30 May 2019) How a quantum computer could break 2048-bit RSA encryption in 8 hours. Available at: https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/ [accessed 15 January 2020].

MIT Technology Review (4 April 2012) How China blocks the Tor anonymity network. Available at: https://www.technologyreview.com/2012/04/04/186902/how-china-blocks-the-tor-anonymity-network/ [accessed 20 September 2020].

Mondaq (31 October 2018) Russian Federation: privacy and security in Russia. Available at: http://www.mondaq.com/russianfederation/x/750216/Data+Protection+Privacy/Privacy+And+Cybersecurity+In+Russia [accessed 16 March 2019].

Mozur, P. (8 July 2018) Inside China's Dystopian Dreams: A.I, shame and lots of cameras, *The New York Times.* Available at: https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html [accessed 24 October 2020].

Murgia, M. (22 November 2018) Study finds half of most popular VPN apps linked to China, *Financial Times.* Available at: https://www.ft.com/content/e5567d8a-ee65-11e8-89c8-d36339d835c0 [accessed 25 November 2018].

Nakashima, E. (21 July 2015) U.S. decides against publicly blaming China for data attack, *The Washington Post.* Available at: https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html?hpid=z1&utm_term=.253069a9fa39 [accessed 2 November 2017].

Nakashima, E. (5 June 2015) With a series of major hacks, China builds a database on Americans, *The Washington Post.* Available at: https://www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fd-d580f1c5d44e_story.html?utm_term=.edb34ba1d249 [accessed 11 January 2018].

NBC News (20 January 2018) Alleged CIA China turncoat Lee may have compromised U.S. spies in Russia too. Available at: https://www.nbcnews.com/news/china/cia-china-turncoat-lee-may-have-compromised-u-s-spies-n839316 [accessed 1 March 2018].

NBC News (25 June 2015) China is 'leading suspect' in OPM hacks, says intelligence chief James Clapper. Available at: http://www.nbcnews.com/tech/security/clapper-china-leading-suspect-opm-hack-n381881 [accessed 1 March 2018].

NBC News (26 August 2013) How Snowden did it. Available at: http://www.nbcnews.com/news/other/how-snowden-did-it-f8C11003160 [accessed March 1 2018].

Nerd4.life (27 March 2020) Players from Russia will not be able to use voice chat in a shooter Valorant. Available at: https://nerd4.life/2020/03/27/players-from-russia-will-not-be-able-to-use-voice-chat-in-a-shooter-valorant/ [accessed 14 December 2020].

New America (30 April 2018) Translation: Xi Jinping's April 20 speech at the National Cybersecuirty and Informatization work conference. Available at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/ [accessed 23 November 2018].

NewsRep (24 March 2015) How technology is changing the future of espionage. Available at: https://thenewsrep.com/40315/technology-changing-future-espionage/#ixzz3imhEq0HG [accessed 23 February 2018].

Norton-Taylor, R. (29 June 2010) Russian spies in UK 'at cold war levels', says MI5, *The Guardian.* Available at: https://www.theguardian.com/world/2010/jun/29/russian-spies-cold-war-levels [accessed 31 November 2017].

NPR (5 January 2020) In China, a new call to protect data privacy. Available at: https://www.npr.org/2020/01/05/793014617/in-china-a-new-call-to-protect-data-privacy?t=1600710014451 [accessed 12 May 2020].

Osborne, H. (2 July 2019) Chinese border guards put secret surveillance app on tourists' phones, *The Guardian.* Available at: https://www.theguardian.com/world/2019/jul/02/chinese-border-guards-surveillance-app-tourists-phones [accessed 14 January 2021].

Paul, K. (18 February 2015) Russia wants to block Tor, but it probably can't, *Vice.* Available at: https://www.vice.com/en_us/article/ypwevy/russia-wants-to-block-tor-but-it-probably-cant [accessed 23 July 2020].

Perera, D. (4 June 2015) Agency didn't encrypt feds' data hacked by Chinese, *Politico.* Available at: https://www.politico.com/story/2015/06/personal-data-of-4-million-federal-employees-hacked-118655 [accessed 23 January 2020].

Philipp, J. (1 March 2016) You're on file: Exclusive inside story on China's database of Americans, *The Epoch Times*. Available at: https://www.theepochtimes.com/youre-on-file-exclusive-inside-story-on-chinas-database-of-americans_1973047.html [accessed 11 January 2018].

Poitras, V. L., Rosenbach, M. & Stark, H. (17 November 2013) GCHQ monitors diplomats' hotel bookings, *Der Spiegel.* Available at: http://www.spiegel.de/international/europe/gchq-monitors-hotel-reservations-to-track-diplomats-a-933914.html [accessed 1 March 2018].

Quartz (18 May 2016) It's official – China is the largest iPhone market in the world. Available at: https://qz.com/687017/its-official-china-is-the-largest-iphone-market-in-the-world/ [accessed 21 January 2018].

Quartz (24 June 2017) Wikileaks: the CIA can remotely hack into computers that aren't even connected to the Internet. Available at: https://qz.com/1013361/wikileaks-the-cia-can-remotely-hack-into-computers-that-arent-even-connected-to-the-internet/ [21 August 2020].

Quartz (24 September 2014) If China really is banning official use of Apple and Samsung phones, here's who benefits. Available at: https://qz.com/270351/if-china-really-is-banning-official-use-of-apple-and-samsung-phones-heres-who-benefits/ [accessed 1 January 2018].

Quartz (6 April 2015) How the New York Times is eluding censors in China. Available at: https://qz.com/374299/how-the-new-york-times-is-eluding-chinas-censors/ [accessed 23 June 2017].

Rapoza, K. (7 January 2019) In Apple loss, how big a deal is China, really?, *Forbes*. Available at: https://www.forbes.com/sites/kenrapoza/2019/01/07/in-apple-loss-how-big-a-deal-is-china-really/#278a659e1aa1 [accessed 3 February 2019].

Reisinger, D. (23 March 2017) WikiLeaks says CIA targeted iPhone supply chain since 2008, *Fortune.* Available at: http://fortune.com/2017/03/23/apple-wikileaks-iphone/ [accessed 1 March 2018].

Reisinger, D. (6 March 2017) Here's how many iPhones are currently being used worldwide, *Fortune*. Available at: http://fortune.com/2017/03/06/apple-iphone-use-worldwide/ [accessed 1 March 2018].

Reuters (13 December 2013) Exclusive: after 'cataclysmic Snowden affair, NSA faces winds of change'. Available at: https://www.reuters.com/article/us-usa-security-nsa/exclusive-after-cataclysmic-snowden-affair-nsa-faces-winds-of-change-idUSBRE9BC0YZ20131213 [accessed 23 June 2017].

Reuters (13 February 2014) NSA memo confirms Snowden scammed passwords from colleagues. Available at: https://www.reuters.com/article/us-usa-security/nsa-memo-confirms-snowden-scammed-passwords-from-colleagues-idUSBREA1C1MR20140213 [accessed March 1 2018].

Reuters (14 July 2017) Russian – American lobbyist met with Trump Jr., Russian lawyer: NBC News. Available at: https://www.reuters.com/article/us-usa-trump-russia-agent/russian-american-lobbyist-met-with-trump-jr-russian-lawyer-nbc-news-idUSKBN19Z189 [accessed 31 November 2017].

Reuters (2 November 2016) Special report – John Brennan's attempt to lead the CIA into the age of cyberwar. Available at: https://uk.reuters.com/article/uk-usa-cia-brennan-specialreport/special-report-john-brennans-attempt-to-lead-the-cia-into-the-age-of-cyberwar-idUKKBN12X1L2 [accessed 11 January 2018].

Reuters (21 November 2011) Russia says Georgia war stopped NATO expansion. Available at: http://in.reuters.com/article/idINIndia-60645720111121 [accessed 30 October 2017].

Reuters (3 March 2020) Chinese cybersecurity company accuses CIA of 11-year-long hacking campaign. Available at: https://www.reuters.com/article/us-china-usa-cia-idUSKBN20Q2SI [accessed 12 May 2020].

Reuters (31 August 2018) Exclusive: U.S. accuses China of 'super aggressive' spy campaign on LinkedIn. Available at: https://www.reuters.com/article/us-linkedin-china-espionage-exclusive/exclusive-u-s-accuses-china-of-super-aggressive-spy-campaign-on-linkedin-idUSKCN1LG15Y [accessed 23 October 2018].

Reuters (7 November 2016) China adopts cyber security law in face of overseas opposition. Available at: https://www.reuters.com/article/us-china-parliament-cyber/china-adopts-cyber-security-law-in-face-of-overseas-opposition-idUSKBN132049 [accessed 21 January 2018].

Reuters (8 September 2017) Putin tells Russia's tech sector: ditch foreign software or lose out. Available at: https://uk.reuters.com/article/russia-it-software/putin-tells-russias-tech-sector-ditch-foreign-software-or-lose-out-idUKL8N1LP4IC [accessed 23 June 2020].

Rogers, K. (1 May 2015) Why was Alan Gross smuggling satellite phones into Cuba?, *Vice.* Available at: https://www.vice.com/en/article/4x379w/why-was-alan-gross-smuggling-satellite-phones-into-cuba [accessed 12 August 2020].

Rogin, J. (26 June 2016) Russia is harassing U.S. diplomats all over Europe, *The Washington Post.* Available at: https://www.washingtonpost.com/opinions/global-opinions/russia-is-harassing-us-diplomats-all-over-europe/2016/06/26/968d1a5a-3bdf-11e6-84e8-1580c7db5275_story.html?utm_term=.dab28978faf0 [accessed 11 January 2018].

Rohrlick, J. (7 September 2016) How OPM bilked a security contractor that confirmed a major hack, *Foreign Policy.* Available at: http://foreignpolicy.com/2016/09/07/how-opm-bilked-a-security-contractor-that-confirmed-a-major-hack-cytech/ [accessed 1 March 2018].

Roth, A. (13 April 2018) Moscow court bans Telegram messaging app, *The Guardian.* Available at: https://www.theguardian.com/world/2018/apr/13/moscow-court-bans-telegram-messaging-app [accessed July 2020].

RT News (13 February 2018) Defense Ministry recommends Russian military quits using social networks – report. Available at: https://www.rt.com/politics/418629-defense-ministry-recommends-russian-military/ [accessed 1 March 2018].

RT News (14 December 2017) Cow-nterintelligence: farmer faces 'spy' charges for wiretapping his cow. Available at: https://www.rt.com/news/413152-armer-spy-cow-gps/ [accessed 21 August 2020].

RT News (19 February 2015) 'Unhackable': Russian firm develops totally surveillance-proof smartphone. Available at: https://www.rt.com/news/233723-russian-phone-security-encryption/ [accessed 1 December 2018].

Russia Today (12 July 2017) Duma passes bill on protection of Russian state data networks. Available at: https://www.rt.com/politics/396096-duma-passes-bill-on-protection/ [accessed 1 March 2018].

Russia Today (25 January 2017) 70m cyberattacks, mostly foreign, targeted Russia's critical infrastructure in 2016 – FSB. Available at: https://www.rt.com/news/374973-cyber-attacks-russian-infrastracture/ [accessed 1 March 2018].

Ryzhkov, V. (16 May 2014) Controlling Russians through travel bans, *The Moscow Times.* Available at: https://themoscowtimes.com/articles/controlling-russians-through-travel-bans-35830 [accessed 11 January 2018].

Sabur, R. (13 December 2017) 'Dirty dossier' on Donald trump is probably credible, says former MI6 boss, *The Telegraph.* Available at http://www.telegraph.co.uk/news/2017/12/13/dirty-dossier-donald-trump-probably-credible-says-former-mi6/?utm_campaign=Echobox&utm_medium=Social&utm_source=Facebook [accessed 10 January 2018].

Sanger, D. E. & Erlanger, S. (March 82014) Suspicion falls on Russia as 'Snake' cyberattacks target Ukraine's government, *The New York Times.* Available at: https://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html [accessed 31 November 2017].

Sanger, D. E. & Schmitt, E. (9 February 2014) Snowden used low-cost tool to best N.S.A, *The New York Times.* Available at: https://www.nytimes.com/2014/02/09/us/snowden-used-low-cost-tool-to-best-nsa.html?hp&_r=1 [accessed 23 July 2017].

Sanger, D. E. (31 July 2015) U.S. decides to retaliate against China's hacking, *The New York Times.* Available at: https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html [accessed 10 January 2018].

Schindler, J. R. (10 October 2017) The trouble with the Steele dossier, *Observer*. Available at: http://observer.com/2017/10/fact-versus-fiction-in-the-steele-dossier-on-donald-trump/ [accessed 31 November 2017].

Schindler, J. R. (11 September 2017) Spies suspect Kremlin is pushing fozens of fake Trump sex tapes, *Observer.* Available at: http://observer.com/2017/11/spy-circles-suspect-kremlin-is-behind-dozens-of-fake-trump-sex-tapes/ [accessed 10 January 2018].

Schindler, J. R. (30 June 2016) Moscow rules of espionage go global – if you think it's KGB, it is: As Russian spies play rough, ignoring Putin's war against the West will only make it nastier, *Observer.* Available at: http://observer.com/2016/06/moscow-rules-of-espionage-go-global-if-you-think-its-kgb-it-is/ [accessed 11 January 2018].

Schmidle, N. (7 August 2017) The U.S. has more to lose than Russia in spy expulsions, *The New Yorker.* Available at: https://www.newyorker.com/news/news-desk/the-us-has-more-to-lose-than-russia-in-spy-expulsions [accessed 10 January 2018].

Sebenius, A. (28 June 2017) Writing the rules of cyberwar, *The Atlantic.* Available at: https://www.theatlantic.com/international/archive/2017/06/cyberattack-russia-ukraine-hack/531957/ [accessed 10 January 2018].

Security Magazine (16 August 2019) China cracking down on data theft caused by mobile apps. Available at: https://www.securitymagazine.com/articles/90732-china-cracking-down-on-data-theft-caused-by-mobile-apps [accessed 12 May 2020].

Seetharaman, D. (3 May 2018) Facebook's double standard on privacy: employees vs. Everyone else, *The Wall Street Journal.* Available at: https://www.wsj.com/articles/facebooks-double-standard-on-privacy-employees-vs-the-rest-of-us-1525383859 [accessed 4 May 2018].

Sevastopulo, D. (22 September 2015) Obama and Xi in deal on cyber espionage, *Financial Times.* Available at: https://www.ft.com/content/0dbcab36-63be-11e5-a28b-50226830d644 [accessed 10 September 2017].

Shachtman, N. (29 June 2010) FBI: spies hid secret messages on public websites, *Wired*. Available at: https://www.wired.com/2010/06/alleged-spies-hid-secret-messages-on-public-websites/ [accessed 23 June 2016].

Shane, S. (3 January 2018) Ex-N.S.A. worker accused of stealing trove of secrets offers to plead guilty, *The New York Times.* Available at: https://www.nytimes.com/2018/01/03/us/politics/harold-martin-nsa-guilty-plea-offer.html [accessed 1 March 2018].

Shane, S., Perlroth, N. & Sanger, D. E. (12 November 2017) Security breach and spilled secrets have shaken the N.S.A. to its core, *The New York Times.* Available at: https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html [accessed 1 March 2018].

Shekhar Shashank (29 December 2015) Security agencies watch 2,000 officers' social media profiles after ISI honey-trap, *Daily Mail India*. Available at: http://www.dailymail.co.uk/indiahome/indianews/article-3378134/Security-agencies-watch-2-000-officers-social-media-profiles-ISI-honey-trap.html [accessed 1 January 2018].

Shubber, K. (13 February 2019) Former US Air Force agent charged with spying for Iran, *Financial Times.* Available at: https://www.ft.com/content/54aa515e-2faa-11e9-8744-e7016697f225 [accessed 24 May 2020].

Shuster, S. (24 March 2014) Putin's fear of texting kept U.S. spymasters in the dark, *Time*. Available at: http://time.com/35932/ukraine-russia-putin-spies-kgb/ [accessed 10 January 2018].

Slate (13 November 2012) Instead of "dead dropping" Petraeus and Broadwell should have used these email security tricks. Available at: https://slate.com/technology/2012/11/petraeus-and-broadwell-should-have-used-pgp-encryption-and-tor-not-dead-dropping-to-secure-affair-emails.html [accessed 16 July 2017].

Slick, S. (4 May 2016) Measuring change at the CIA, *Foreign Policy.* Available at: http://foreignpolicy.com/2016/05/04/measuring-change-at-the-cia/ [accessed 11 January 2018].

Solon, O. (13 September 2017) US government bans agencies from using Kaspersky software over spying fears, *The Guardian.* Available at: https://www.theguardian.com/technology/2017/sep/13/us-government-bans-kaspersky-lab-russian-spying [accessed 10 January 2018].

Statista (22 July 2019) Global VPN usage reach 2018, by region. Available at: https://www.statista.com/statistics/306955/vpn-proxy-server-use-worldwide-by-region/ [accessed 21 March 2020].

Stein, J. (22 May 2017) Chinese counterspies roiling U.S. intelligence operations in Beijing, *Newsweek.* Available at: http://www.newsweek.com/chinese-counterspies-roiling-us-intelligence-operations-613393 [accessed 11 January 2018].

Stein, J. (3 August 2017) How Russia is using LinkedIn as a tool of war against its U.S. enemies, *Newsweek.* Available at: https://www.newsweek.com/russia-putin-bots-linkedin-facebook-trump-clinton-kremlin-critics-poison-war-645696 [accessed 23 October 2018].

Stein, J. (3 July 2015) The Russian spy who came in through the email, *Newsweek.* Available at: https://www.newsweek.com/russian-spy-through-email-312104 [accessed 10 June 2017].

Stein, J. (31 March 2017) Why the CIA is increasingly worried about China's moles, *Newsweek*. Available at: http://www.newsweek.com/cia-chinese-moles-beijing-spies-577442 [accessed 10 January 2018].

Stein, J. (4 December 2012) CIA's secret fear: high-tech border checks will blow spies' cover, *Wired*. Available at: https://www.wired.com/2012/04/cia-spies-biometric-tech/ [accessed 11 January 2018].

Sudakov, D. (2 May 2017) Russia may block WhatsApp, Viber, Telegram even tomorrow, *Pravda*. Available at: http://www.pravdareport.com/business/companies/02-05-2017/137639-messaging_service_russia-0/ [accessed 31 January 2018].

Surveillance Self-Defense (30 October 2015) The problem with mobile phones. Available at: https://ssd.eff.org/en/module/problem-mobile-phones [accessed 1 January 2018].

Taiwan News (15 April 2020) China to ban online gaming, chatting with foreigners outside Great Firewall: report. Available at: https://www.taiwannews.com.tw/en/news/3916690 [accessed 9 May 2020].

Tassi, P. (14 November 2015) How ISIS terrorists may have used PlayStation 4 to discuss and plan attacks [updated], *Forbes.* Available at: https://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/#5b4eb7b70554 [accessed 14 March 2019].

Tatlow, D. K. (2 November 2014) China approves security law emphasizing counterespionage, *The New York Times.* Available at: https://www.nytimes.com/2014/11/03/world/asia/china-approves-security-law-emphasizing-counterespionage.html?ref=asia [accessed 11 January 2018].

Tech Crunch (25 November 2015) China punishes VPN users in its rural northwest by cutting their mobile service. Available at: https://techcrunch.com/2015/11/25/china-punishes-vpn-users-in-its-rural-northwest-by-cutting-their-mobile-service/?_ga=2.42157157.1785373780.1543256229-223957389.1543256229 [accessed 20 June 2017].

Tech Crunch (27 October 2013) Meet Telegram, a secure messaging app from the founders of VK, Russia's largest social network. Available at: https://techcrunch.com/2013/10/27/meet-telegram-a-secure-messaging-app-from-the-founders-of-vk-russias-largest-social-network/ [accessed 5 February 2018].

Tech Crunch (5 August 2010) Eric Schmidt: every 2 days we create as much information as we did up to 2003. Available at: https://techcrunch.com/2010/08/04/schmidt-data/ [accessed 16 March 2019].

Tech Crunch (7 March 2017) Russia says 'nyet,', continues LinkedIn block after it refuses to store data in Russia. Available at: https://techcrunch.com/2017/03/07/russia-says-nyet-continues-linkedin-block-after-it-refuses-to-store-data-in-russia/ [accessed 31 January 2018].

Tech Native (10 July 2018) Retaliatory hacking has returned – will states ever learn? Available at: https://www.technative.io/retaliatory-hacking-has-returned-will-states-ever-learn/ [accessed 12 May 2020].

TechCrunch (17 November 2017) LinkedIn is now officially blocked in Russia. Available at: https://techcrunch.com/2016/11/17/linkedin-is-now-officially-blocked-in-russia/ [accessed 31 January 2018].

TechNode (17 March 2016) Behind the scenes: here's why your VPN is down in China. Available at: https://technode.com/2016/03/17/behind-scenes-heres-vpn/ [accessed 20 November 2017].

Telestial (8 November 2017) Countries where satellite phones are banned or restricted. Available at: https://blog.telestial.com/2017/11/countries-where-satellite-phones-banned-or-restricted/ [accessed 1 January 2018].

The Aspen Institute (29 July 2016) A candid conversation with the Director of the Central Intelligence Agency, Youtube. Available at: https://www.youtube.com/watch?v=TRCUO7-lbUE [accessed 11 January 2018].

The Cipher Brief (30 January 2016) Espionage and social media. Available at: https://www.thecipherbrief.com/column_article/espionage-and-social-media [accessed 1 January 2018].

The Conversation (20 March 2017) Tor upgrades to make anonymous publishing safer. Available at: https://theconversation.com/tor-upgrades-to-make-anonymous-publishing-safer-73641 [accessed 23 July 2020].

The Daily Dot (29 February 2016) Russia's rise to cyberwar superpower. Available at: http://www.dailydot.com/layer8/russia-cyberwar-cyberattack-dnc-breach-history/ [accessed 31 November 2017].

The Diplomat (23 January 2016) China's comprehensive counter-terrorism law. Available at: https://thediplomat.com/2016/01/chinas-comprehensive-counter-terrorism-law/ [accessed 11 January 2018].

The Hacker News (22 June 2017) Brutal Kangaroo: CIA-developed malware for hacking air-gapped networks covertly. Available at: https://thehackernews.com/2017/06/wikileaks-Brutal-Kangaroo-airgap-malware.html [accessed August 21].

The Intercept (25 April 2016) Spy chief complains that Edward Snowden sped up spread of encryption by 7 years. Available at: https://theintercept.com/2016/04/25/spy-chief-complains-that-edward-snowden-sped-up-spread-of-encryption-by-7-years/ [accessed 23 May 2020]

The Register (`7 July 2020) Seven 'no log' VPN providers accused of leaking – yup, you guessed it – 1.2TB of user logs onto the Internet. Available at: https://www.theregister.com/2020/07/17/ufo_vpn_database/ [accessed 20 September 2020].

The Sun (19 January 2012) UK admits using fake rock to spy. Available at: https://www.thesun.co.uk/archives/news/314694/uk-admits-using-fake-rock-to-spy/ [accessed 20 October 2020].

The Telegraph (14 May 2013) CIA agent 'detained in Moscow': his 'letter' in full. Available at: http://www.telegraph.co.uk/news/worldnews/europe/russia/10056972/CIA-agent-detained-in-Moscow-his-letter-in-full.html [accessed 16 July 2017].

The Telegraph (20 May 2017) British and US spies at risk after WikiLeaks publishes top-secret CIA spyware document. Available at: https://www.telegraph.co.uk/news/2017/05/20/british-us-spies-risk-wikileaks-publishes-top-secret-cia-spyware/ [accessed 1 March 2018].

The Telegraph (27 September 2017) Russia threatens to ban Facebook in election year. Available at: http://www.telegraph.co.uk/news/2017/09/27/russia-threatens-ban-facebook-election-year/ [accessed 31 January 2018].

The Verge (11 January 2018) Skype starts testing new 'private conversations' with end-to-end encryption. Available at: https://www.theverge.com/2018/1/11/16878596/microsoft-skype-end-to-end-encryption-private-conversations [accessed 5 February 2018].

The Verge (13 June 2017) Apple is building its first China-based data center per new cybersecurity law. Available at: https://www.theverge.com/2017/7/13/15964220/apple-china-data-center-icloud-new-cybersecurity-law-guizhou [accessed 24 January 2018].

The Verge (17 April 2018) Russia's Telegram ban is a big, convoluted mess. Available at: https://www.theverge.com/2018/4/17/17246150/telegram-russia-ban [accessed 20 November 2018].

The Verge (24 August 2017) The CIA built a fake software update system to spy on intel partners. Available at: https://www.theverge.com/2017/8/24/16197694/cia-fake-software-update-hacking-WikiLeaks-vault-7 [accessed 11 January 2018].

The Verge (25 October 2018) How China complicates Apple's chest-thumping about privacy. Available at: https://www.theverge.com/2018/10/25/18020508/how-china-complicates-apples-chest-thumping-about-privacy [accessed 21 December 2018].

The Verge (7 November 2017) China's education group released a cartoon encouraging kids to embrace counterespionage. Available at: https://www.theverge.com/2017/11/7/16617494/china-national-security-spying-propaganda-cartoon-education [accessed 15 January 2021].

Troianovski, A. (16 May 2013) Social media pose new riddle for CIA, *The Wall Street Journal.* Available at: https://www.wsj.com/articles/SB10001424127887323398204578487173173371526 [accessed 11 January 2018].

WalesOnline (20 March 2014) The carnage in Crimea during World War II has shaped Putin's response to Ukraine crisis, argues Welsh historian. Available at:

http://www.walesonline.co.uk/news/wales-news/memories-carnage-crimea-during-world-6851251 [accessed 31 October 2017].

Walker, S. (17 May 2016) Face recognition app taking Russia by storm may bring end to public anonymity, *The Guardian.* Available at: https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte [accessed 11 January 2018].

Walker, S. (31 January 2017) Russia accuses cybersecurity experts of treasonous links to CIA, *The Guardian.* Available at: https://www.theguardian.com/world/2017/jan/31/russian-cybersecurity-experts-face-treason-charges-cia [accessed 10 January 2018].

Waterman, S. (14 June 2013) NSA leaker Ed Snowden used banned thumb-drive, exceeded access, *The Washington Times.* Available at: https://www.washingtontimes.com/news/2013/jun/14/nsa-leaker-ed-snowden-used-banned-thumb-drive-exce/ [accessed 1 March 2018].

Watkins, A. (1 June 2017) Russia escalates spy games after years of US neglect, *Politico.* Available at: https://www.politico.eu/article/russia-escalates-spy-games-after-years-of-us-neglect/ [accessed 24 October 2017].

Watkins, A. (10 November 2017) China grabbed American as spy wars flare, *Politico.* Available at: https://www.politico.com/story/2017/10/11/china-spy-games-espionage-243644 [accessed 11 January 2018].

Wong, E. (27 August 2019) How China uses LinkedIn to recruit spies abroad, *The New York Times.* Available at: https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html [accessed 1 December 2020].

Yahoo News (13 January 2018) 'Very high level of confidence' Russia used Kaspersky software for devastating NSA leaks. Available at: https://finance.yahoo.com/news/experts-link-nsa-leaks-shadow-brokers-russia-kaspersky-144840962.html?guccounter=2 [accessed 1 March 2018].

Yahoo News (2 November 2018) The CIA's communications suffered a catastrophic compromise. It started in Iran. Available at: https://in.news.yahoo.com/cias-communications-suffered-catastrophic-compromise-started-iran-090018710.html?guccounter=1 [accessed 3 November 2018].

Yahoo News (2 September 2019) Revealed: how a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran. Available at: https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAH0unYTO_3FCbroLyqk4XhbV4hBU4AEVLdj8MwLshOYraeKSxB59cqQ6WgHmk7rpBG3jDdbajDmEtwLJirKfyapCsL1pN1-2Yw2RNsn_zXdL9XngDaCj958MNSfHhf4eIAlnx5pgkJgcWjTMjL6SSgbzhurP2W2t-P_17HSClU7C&_guc_consent_skip=1597675156 [accessed 21 August 2020].

Yang, Y. (30 May 2017) China's cybersecurity law rattles multinationals, *Financial Times.* Available at: https://www.ft.com/content/b302269c-44ff-11e7-8519-9f94ee97d996 [accessed 1 March 2018].

Yin, C. (10 March 2015) More 'eyes' fight crime in crowds, *China Daily*. Available at: http://www.chinadaily.com.cn/china/2015-10/05/content_22091634.htm [accessed 11 January 2018]

Yixue W. (5 September 2014) Guard secrets against spy net, *China Daily.* Available at: http://www.chinadaily.com.cn/opinion/2014-05/09/content_17494978.htm [accessed 12 August 2017].

ZDNet (30 July 2020) EU sanctions China, Russia, and North Korea for past hacks. Available at: https://www.zdnet.com/article/eu-sanctions-china-russia-and-north-korea-for-past-hacks/ [accessed 24 August 2020].

Zetter, K. (2 May 2015) Health insurer anthem is hacked, exposing millions of patients' data, *Wired*. Available at: https://www.wired.com/2015/02/breach-health-insurer-exposes-sensitive-data-millions-patients/ [accessed 19 March 2019].

Zetter, K. (3 July 2014) The NSA is targeting users of privacy services, leaked codes shows, *Wired*. Available at: https://www.wired.com/2014/07/nsa-targets-users-of-privacy-services/ [accessed 1 March 2018].

Zetter, K. (3 March 2016) Inside the cunning, unprecedented hack of Ukraine's power grid, *Wired*. Available at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ [accessed 31 November 2017].

Zetter, K. (9 December 2011) The return of the worm that ate the Pentagon, *Wired*. Available at: https://www.wired.com/2011/12/worm-pentagon/ [accessed 31 November 2017].

Zhou, M. (2 November 2017) Fingerprinting of foreign visitors gets started at Shenzhen's Bao'an Airport, *China Daily*. Available at: http://www.chinadaily.com.cn/china/2017-02/11/content_28168119.htm [accessed 11 January 2018]

Zhou, V. (6 November 2017) 'Grandpa, what are spies?' Cartoon urges Chinese children to be on alert: National Security Law requires national security to be part of children's education, *South China Morning Post*. Available at: https://www.scmp.com/news/china/policies-politics/article/2118553/grandpa-what-are-spies-cartoon-urges-chinese-children [accessed 16 December 2017].

Online videos

Bob Kovacs (3 March 2010) CIA gadgets and techniques with Bob Wallace – in HD, Youtube. Available at: https://www.youtube.com/watch?v=vQ7K52cvpyA [accessed 10 January 2018].

University of Delaware (21 September 2012) Human Intelligence in the digital age: global agenda 2012, Youtube. Available at: https://www.youtube.com/watch?v=bfIxarRLMDo [accessed 23 January 2016].

Permanent Select Committee on Intelligence (10 September 2015) World Wide Cyber Threats Hearing. Available at: https://www.youtube.com/watch?v=Q3aG0CtZbU4 [accessed 31 October 2017].

Parliamentlive.tv (8 March 2016) Russia: Implication for UK defence and security. Available at: http://parliamentlive.tv/Event/Index/f221826a-b5dd-4200-b00b-1bdf9d7a7c0e [accessed 10 January 2018].

The Aspen Institute (29 July 2016) A candid conversation with the Director of the Central Intelligence Agency, Youtube. Available at: https://www.youtube.com/watch?v=TRCUO7-lbUE [accessed 11 January 2018].

GW Center for Cyber and Homeland Security (21 September 2016) CIA-GW intelligence conference: Panel on the view from foreign intelligence chiefs, Youtube. Available at: https://www.youtube.com/watch?v=yefBv7Q3sv0 [accessed 11 January 2018].

Dissertations and theses

Morozova, O. ‘Russian politics and deception: The Kremlin’s reaction to the revolutions of 2004-2014 and information warfare in Russia-Ukraine relations’, MA Russian and Eurasian Studies, Leiden University, 2017.

Streeter, D. C. ‘Biometrics and intelligence asset protection: Biometric technology and its impact on counterintelligence and intelligence’, Liberty University Helm’s School of Government, 2013.

APPENDIX 1:

1- **Remarks of Deputy Director David S. Cohen Central Intelligence Agency as Prepared for Delivery on "The CIA of the Future," LaFeber-Silbey Endowment in History Lecture, Cornell University - September 17, 2015**

Dean Ritter, Professor LaFeber, Professor Silbey, fellow Cornellians:

It is a tremendous honor, and a great thrill, to join you this afternoon—just over 30 years since I graduated from this spectacular University—to deliver the Fall 2015 LaFeber-Silbey Endowment in History Lecture.

It is more than a bit daunting to be delivering a lecture in a series named for two of Cornell's greatest professors, Walter LaFeber and Joel Silbey, who as scholars offered invaluable insights into the history of American foreign and domestic policy, and who, as teachers, contributed immensely to the education of generations of Cornell students.

I am one of those lucky Cornell students. In the spring of my junior year, I took Professor LaFeber's legendary course, "American Foreign Policy from 1914 to the Present." I still have my notes from the class. Looking them over, I can't believe that I once knew all those things. Unfortunately for me, "present" only went up to the early Reagan Administration—I could use some notes on more recent times.

It was Professors like Walter LaFeber and Joel Silbey—some of whom are here today—who first sparked my interest in foreign policy and national security.

My senior thesis was a critique of the Carter Administration's reaction to the 1979 Soviet invasion of Afghanistan. I argued that the Carter Administration mistakenly viewed the Soviet invasion as a failure of American deterrence, when, instead, the Soviets invaded principally because of domestic political imperatives unrelated to a US-Soviet cost-benefit calculation.

And after I graduated, I spent a year here in Ithaca, working on a project studying the potential for a crisis between United States and the Soviet Union to spin out of control due to mutual misunderstandings or the inability to exercise effective command and control in a crisis situation.

I describe these two projects not because I was a great national security scholar—far from it. But what ties these two projects together is that both, at bottom, implicitly recognize that solid intelligence on the plans, intentions and motivations of one's adversary is both critical and hard to obtain. Fending off misunderstandings and misperceptions with real insight into a foreign leader's thinking and a foreign power's plans, into what can affect an adversary's decisionmaking—that is hard, but it is essential if we are to effectively advance our foreign policy goals and protect our national security.

At CIA, where I now have the privilege of serving as Deputy Director, our mission is to supply just that kind of insight—to collect, analyze, and produce timely and accurate foreign intelligence that allows US policymakers to see the world as it truly is—so that the decisions they take are as fully informed as possible. This has been core to CIA's mission since its founding in 1947.

One interesting window into this effort opened yesterday, with the release of nearly 2,500 previously classified intelligence documents prepared for Presidents Kennedy and Johnson. These documents comprise the daily Presidential intelligence briefings spanning from the beginning of the Kennedy administration to the end of the Johnson administration, and reflect the Agency's early efforts to provide our "first customer" with useful intelligence reporting and analysis on a range of critical issues of the day, including the Cuban Missile Crisis, the Soviet invasion of Czechoslovakia and, of course, Vietnam.

The documents bear witness to some of the countless contributions CIA has made to the security of our country over the past 68 years. But we know that if we are to continue fulfilling our responsibilities—and if we are to do an even better job in the future—we can't afford to rest on our laurels.

Which brings me to the topic of my talk today—the CIA of the future. Earlier this year, my boss, CIA Director John Brennan, announced a comprehensive strategic modernization program for the Agency. The impetus for the modernization effort is two-fold: first, the marked increase in the range, diversity, complexity and immediacy of the national security issues confronting our policymakers; and second, the unprecedented pace and impact of technological advancements. The changes we are implementing are designed to ensure that the Agency, which operates today at very high level, is even more integrated, more agile, and ultimately more effective in tackling the complex challenges of an increasingly volatile world in the years ahead.

Today, I want to focus on three elements that are central to this plan.

The first, the collection of human intelligence, is something that has always been at the heart of CIA's mission. Although the global security landscape is always evolving, one constant is the need to understand the plans and intentions of our adversaries—something that well-executed espionage is especially good at revealing. I'll spend a few minutes describing how we collect human intelligence and why it will be a remain a key piece of the CIA of the future.

The second key element in the CIA of the future is our creation of a new entity within the CIA that focuses specifically on the cyber and digital domain. By necessity, we—like every other institution—operate today in the digital world. As I'm sure you can imagine, for an intelligence agency, this presents unique challenges and opportunities. I'll spend a few minutes describing how we will better protect our Agency and our officers in this new environment, and how we will leverage the digital domain to fulfill our intelligence collection and analysis responsibilities.

And finally, I will discuss our enhanced efforts to promote a diverse and inclusive workforce. Although we are by no means unique in this regard, the imperative—from both a moral and a mission perspective—of developing a broadly diverse workforce,

top-to-bottom and in all our constituent parts, is unmistakable. And so I'll conclude with a few words about what we are doing to improve our performance on attracting, developing, and promoting a diverse and inclusive workforce.

Snapshot of The World Today

Before turning to the CIA of the future, let me begin by briefly describing some of what our analysts see when they look at the world today.

Most importantly, they see a world that is more unstable than it has been for several decades.

In the past three years, there have been more outbreaks of instability than at any time since the collapse of the Soviet Union, matching the rate we saw during decolonization in the 1960s.

This has not just been a period of protests and government change, but of violent insurgency and, in particular, of breakdowns in the ability of many states to govern.

At the state-to-state level, intensifying rivalry and competition—such as between Iran and Saudi Arabia in the Middle East, and among China, Japan, and the Koreas in East Asia—and challenges from China and Russia to US leadership in the international order, are inhibiting cooperative solutions to this historic instability.

We see clear examples of rising volatility in places such as Ukraine, Syria, Iraq, Yemen, Libya, Afghanistan and Nigeria. The human toll of the conflicts in these countries is reflected on the front pages of our newspapers, and it is confirmed by the UN's recent announcement that the number of refugees and internally displaced persons in the world today is the highest it has been since World War II.

Beyond violent conflicts, there are a number of places where tension is running high, such as on the Korean peninsula, in the South China Sea, in South Sudan, in Burundi, and on the border between Pakistan and India, to name just a few.

When our analysts look for the deeper causes of this rising instability, they see a range of factors. Let me touch upon a few of them.

First, the ideas, institutions, and states that have formed the foundation of the post-Cold War system, and have delivered at least a modicum of governance, service, and security to often multi-ethnic populations, are under stress. Nowhere is this more apparent than in the brutal extremism of the so-called Islamic State in Iraq and the Levant (ISIL), which seeks to erase the borders—and, tragically, the ancient communities—of Syria and Iraq.

At the same time, democratic governance is under siege. For the ninth consecutive year, Freedom House in 2014 reported more declines than gains in the quality of democracy worldwide. Worsening ethno-sectarian and socioeconomic strains are contributing to the trend. So, too, does the rise of a more sophisticated form of authoritarianism that

forgoes brute force and heavy-handed propaganda in favor of technology-enabled media manipulation, ubiquitous surveillance, criminalization of dissent, and controlled elections.

Next, we see that some of the world's largest economies—particularly in Europe and Japan—have struggled to achieve strong, sustained growth in the wake of the 2008 financial crash and Eurozone crisis. And as we have witnessed over the summer, China's economy, which once seemed to have endless potential for growth, is slowing.

Elsewhere, growing pessimism about future economic prospects is fueling instability in many developing societies. Regions with burgeoning youth populations, such as the Arab world, have been unable to achieve the growth needed to reduce high unemployment rates, let alone create the jobs necessary to satisfy an expanding labor force.

In many places, perceptions of growing inequality have resulted in more assertive street politics and populism. At the same time, slower growth has left these nations with fewer resources to devote to economic, humanitarian, and peacekeeping assistance to address these challenges.

Finally, there is both promise and peril in the defining breakthrough of our time—the rapid development and diffusion of communications and information technology.

News and knowledge have never flowed so freely and quickly, but the same is true for misinformation and malign ideologies. An entirely new realm for human interaction—bridging continents, classes, and cultures—is bringing the world closer together, even as criminals, terrorists, and rogue regimes seek to exploit it for their own purposes. ISIL's sophisticated use of Twitter and other social media platforms is a perfect example of the malign use of these technologies.

Taken together, all of these challenges—rising instability, rapidly advancing technology, an ever-growing list of security threats—mean that in many ways our portfolio at CIA is more complicated and more demanding today than it has ever been.

So what are we at the CIA doing about it? How will the CIA of the future help our policymakers make sense of this world, understand the threats and see the opportunities?

Collection of Human Intelligence

First of all, we are working to ensure that the CIA is as effective and productive as possible in its core intelligence gathering mission—the collection of human intelligence, HUMINT, or what is more popularly known as spying.

I'm sure many of you have heard the claim that CIA is less focused on espionage than it used to be, and that in the years since 9/11, we have become an agency devoted above all to paramilitary activities. This claim is seriously misguided.

CIA is first and foremost an espionage organization engaged in the collection and analysis of foreign intelligence. We always have been. And any discussion of what CIA will look like in the future must begin there to take account of all of CIA's capabilities. For now, I'd like to focus on that first piece—the collection of HUMINT.

In the simplest terms, HUMINT is intelligence collected by human beings—by spies operating on the ground—as opposed to intelligence gathered through technical means, like a satellite or a microphone. It involves recruiting people—such as members of a foreign government, or individuals with inside access to a weapons proliferation network—and convincing them to collect and convey valuable information for us.

Let me emphasize up front that CIA collects only foreign intelligence—that is, information relating to foreign governments, foreign organizations, foreign persons, or international terrorists.

And contrary to what you may have seen on "Homeland," CIA does not undertake foreign intelligence collection in the United States to acquire information concerning the domestic activities of US citizens. Our efforts are focused overseas, on identifying threats and opportunities linked to foreign individuals, governments and organizations outside our borders.

As you might imagine, collecting human intelligence is a complicated endeavor, and doing it well requires years of training. To be a CIA case officer, you must master the basic tradecraft of espionage, things like how to evade surveillance, or how to elicit information from a source.

You often need foreign language skills, along with a deep understanding of the culture where you have been assigned to operate. You also need expertise in the target you've been given, whether it's a terrorist group, a drug cartel, an illicit weapons network, or the inner workings of a foreign government.

And perhaps most importantly, you have to understand people—their motivations, their interests, their dreams and ambitions, their vulnerabilities, their grudges—really, everything that makes them tick.

The art of collecting human intelligence—how we go about recruiting and handling our sources—is endlessly fascinating. But there are a few persistent myths that I'd like to address, because they represent a fundamental misunderstanding of how human intelligence works, and how the practice of collecting HUMINT in the future will operate.

First, contrary to what you may have seen in the movies, CIA's case officers do not spend most of their time at cocktail parties and diplomatic functions, canvassing the gilded salons of exotic foreign capitals.

In today's world—and especially tomorrow's—the cocktail circuit does not make for particularly good HUMINT hunting. As one of my predecessors, Michael Morell, used to say: Al-Qa'ida and ISIL are not on the cocktail circuit. And so neither are we.

Nor do our best recruits simply walk into our offices, without any enticement from us, and volunteer information. It is true that walk-ins can be extremely valuable. Indeed, over the years, they have provided us with critical insights on a host of targets. But our case officers can't just sit in their offices and wait for sources to fall into our laps.

More typically, CIA officers are out developing sources, a task that can take months and sometimes years of painstaking effort. The case officer must identify the people who have access to the information she is seeking. She then needs to find a way to meet them, build a relationship with them and earn their trust. Then comes the recruitment phase—the effort to persuade them to help our government, whether for money; because of ideological affinity for the United States or loathing of their home country; due to fear of compromise; to feed an undernourished ego; or for the sheer thrill of it.

Developing assets is difficult and often dangerous work. There is always a possibility that the source our officer is pursuing is what we call a dangle, someone deliberately offered up by an adversary to feed us false information, to manipulate us, or to help them identify our officers. In fact, every meeting with a source is fraught with uncertainty, especially early encounters when we have yet to take the full measure of the potential source's character and motivations.

And the uncertainty never really goes away, because even sources with a long track record of acting in good faith can be a double-agent from the start, or caught and turned against us. So when our officers step out into the streets to meet with a source, they go into the encounter knowing that anything can happen—that they may be detained, harassed, or even attacked. In many cases, especially in the more lawless regions of the globe, they are truly putting their lives on the line.

About five years ago, we were reminded just how dangerous human intelligence collection can be. In December 2009, a group of Agency officers gathered to meet with a source at a desolate outpost in southeastern Afghanistan near the border with Pakistan—a place called Khost.

The source seemed to be an intelligence goldmine. For months, he had been providing us with inside information on al-Qa'ida—good information that we were able to verify independently. But it turned out that the source was a double agent.

When he arrived for his meeting with our officers, the source detonated a bomb hidden inside his clothing, killing seven of our officers and wounding six others. It was one of the bloodiest attacks ever against Agency personnel.

In the lobby of our Headquarters in Langley we have a Memorial Wall. On that wall are 113 stars, one for each CIA officer killed in the line of duty since our founding in 1947, including seven for the officers killed in Khost in 2009.

So, collecting human intelligence is not a profession for the faint of heart. It demands courage, discipline, guile, and wit. It is and always will be a very risky business. But it has to be done. Often, it is the only way to get the information and insight our government needs to safeguard our country.

Technical forms of intelligence, such as satellite imagery, can tell you a lot about things that are large or hard to hide, such as the size of a nation's army, or whether a country is testing a new missile system. But they are not always well-suited to telling you what a government plans to do with those things.

Likewise, intercepted communications can reveal what someone has said or written, but the topics very well may be irrelevant or the communications impossibly difficult to comprehend without knowing the context. As Richard Helms, one of our former Directors, once said: "Gadgets cannot divine man's intentions."

What makes human intelligence so valuable is that, in the give and take between our officers and their sources, HUMINT can provide that critical insight into our adversaries' plans and intentions—it can help you understand how your adversaries think, and what they might do next, because our officers can engage directly with their sources, asking the motivational questions we need answered to inform the President and his advisors as they formulate policy.

Looking to the future, there is little doubt that HUMINT will continue to play a critical role in revealing the plans, motivations, intentions, and capabilities of an increasingly diverse array of state and non-state adversaries. Indeed, the importance of HUMINT in our overall intelligence collection efforts is only likely to grow. Let me offer a few reasons why.

First, HUMINT penetrations will be that much more important as we increasingly confront threats from non-state actors—whose challenge to our security doesn't involve traditional warfare and whose capabilities can't be measured by counting tanks or missiles. A well-placed source inside a terrorist organization, a weapons proliferation network or a criminal gang can yield enormously valuable intelligence that simply cannot be acquired through any other means.

Second, largely because of unauthorized disclosures revealing how the US Intelligence Community conducts signals intelligence, some of our most potent and dangerous adversaries—state and non-state actors alike—have become savvier in thwarting technical methods of collection.

As Director of National Intelligence Jim Clapper recently said, these unauthorized disclosures have "done huge damage for our collection…make no mistake about it." That loss of collection puts even more of a premium on HUMINT.

Third, our adversaries are increasingly trying to steal our secrets. One of CIA's core missions is counter-intelligence—that is, defending the United States against the intelligence collection efforts of others. One surefire way to accomplish this task is to collect intelligence on the efforts underway by our adversaries to penetrate the US government. This is classic spy v. spy stuff—and there is no reason to expect that it will abate in the future.

So, in conjunction with the modernization effort, we are taking several steps to ensure that CIA's HUMINT enterprise continues to thrive in the future. Perhaps most notably, we are emphasizing collaboration—within the CIA, across the intelligence community and with allied intelligence services overseas. We are convinced that effectively

addressing the highly complex challenges we face today, and will face tomorrow, demands a team approach to our human-intelligence mission.

Within the CIA, we are creating ten dedicated Mission Centers—six focused on the world's regions, four on topics of great importance—that span the work of the Agency. Within each Mission Center, we will bring together specialists from all our key disciplines: our case officers who collect intelligence; our analysts who draft finished intelligence papers; our scientists and technologists who provide the tools that enable our collection; and our support officers who sustain our operations at home and overseas.

This cross-discipline collaboration will help ensure that we optimize our HUMINT collection to produce intelligence useful in answering the analytic questions our policymakers need answered, while leveraging CIA's analytical and technical expertise to support the HUMINT operations we undertake.

Similarly, we are working to enhance our partnerships with organizations across the Intelligence Community, including other HUMINT collectors and specialized analysts. The advantages of this collaborative approach are especially clear with interdisciplinary challenges, which depending on the issue can call on the skills of political analysts, financial experts, counterterrorism specialists, military professionals, oil market experts, and so on.

And overseas, our work with foreign intelligence services opens windows on regions and issues that might otherwise be closed to us. Today's world is so complex, and the challenges so widely dispersed across the globe, that no intelligence organization can cover them alone. The only way we can be successful in carrying out our global mission is by working with foreign partners.

On countless occasions, our cooperation with foreign liaison has quietly achieved significant results. Working together, we have disrupted terrorist plots, broken vicious insurgencies, intercepted transfers of dangerous weapons and technology, and brought international criminals to justice, among many other accomplishments. And as CIA assists many of these services in building their human-intelligence collection capability while insisting that, in the process, they respect fundamental human rights, we can count even more on their partnership in helping us expand our own collection efforts around the globe.

The New Directorate of Digital Innovation

So that is the first element—HUMINT in the CIA of the future. I'd like to turn now to the second key element of our plan to modernize the CIA—the creation of the Directorate of Digital Innovation, or the DDI.

As I noted earlier, our modernization effort was spurred, in part, by the recognition that the Agency is increasingly operating in, and responding to threats from, the digital domain.

Shortly after Director Brennan arrived at the CIA in March 2013, he recognized that the rapidly changing digital domain stood out as an area that needed special attention. And when he asked a group of our senior officers to offer suggestions on the future of the Agency, they came back with the same advice: As an Agency, we were not well-prepared to leverage the opportunities of emerging digital technology. The consensus was clear—as an Agency, we needed to adapt better to the digital domain.

And while that may sound a bit obvious—after all, what organization doesn't have to adapt to the digital world?—it's a much more complicated proposition for CIA. For example, as proud as we are of the cutting-edge clandestine technology we've developed for use in the field, our officers still can't bring smartphones into work, and we've only recently figured out how to allow some personnel to take notes in a meeting on a laptop instead of with a pen and paper.

This isn't simply resistance to change. As an intelligence agency working with our country's most sensitive secrets, we need to operate in a secure environment, protected from the prying eyes of hostile intelligence services. That considerably complicates how we operate in the digital domain.

Still, notwithstanding our well-founded concerns, we understood that we needed to adapt to the new reality. So to speed the Agency-wide embrace of the digital domain, we created the Directorate of Digital Innovation—the first new Directorate since 1963, when we set up the Directorate of Science to Technology to build our spy gadgets.

The DDI, which will begin operation October 1st, is charged with ensuring that we approach the digital domain in a well-coordinated, determined and assertive fashion, and that we develop and adopt digital solutions in all aspects of our work—from collection to analysis to our internal business practices.

Let me describe just some of the DDI's responsibilities.

As we go about collecting HUMINT, the DDI will help our clandestine officers maintain effective cover in the modern, digital world. For our case officers, the cyber age is very much a double-edged sword. While digital footprints may enable us to track down a suspected terrorist, this "digital dust" can also leave our officers vulnerable.

Think about it: Every one of us leaves a digital trail that an enterprising foreign intelligence service can try to follow—credit card transactions; car rentals; internet searches and purchases; the list goes on and on because, in a sense, we all "live" in a digital world. Our interactions, transactions, and communications are increasingly performed or stored in a digital form.

From the standpoint of a clandestine officer seeking to create and maintain her cover—perhaps the most fundamental element of espionage—this can pose a real challenge. We must find ways to protect the identity of our officers who increasingly have a digital footprint from birth. Likewise, since having no digital trail can raise suspicions too, we also have to figure out how to create digital footprints to support cover identities. Within this digital world, the DDI, collaborating with other components in the Agency, will work to ensure that our officers can continue to operate clandestinely.

The DDI also will be deeply involved in our efforts to defend the Agency against foreign cyber attacks. As I am sure you are all aware, cyber attacks against the U.S. government—like those against businesses, universities, and organizations all across the country—are increasing in frequency, scale, sophistication, and severity of impact.

One of the DDI's key responsibilities is developing the policies, technologies and protocols to better defend the Agency against these attacks. Its cyber threat analysts, who are experts in hackers' tools and techniques, work with highly classified intelligence on the plans, intentions and capabilities of an ever-expanding assortment of malicious cyber actors.

And along with others in the intelligence community as well as our colleagues from the Department of Homeland Security and the FBI, these analysts defend our networks against attacks and protect our highly sensitive data from exploitation.

The DDI's mandate, however, is not simply to defend the Agency and its officers in the digital world. Equally importantly, the DDI will help us harness the digital domain to provide policymakers the insight they require.

In that vein, the DDI will oversee the efforts of our Open Source Enterprise, a unit dedicated to collecting, analyzing and disseminating publicly available information of intelligence value. The fact is, information does not have to be secret to be valuable. More and more, information relevant to US intelligence requirements is openly available on foreign web sites and in social media. Knowing what's out there for the taking allows us to better focus our risky and expensive human collection efforts on the key national security questions that cannot be answered in any other way. And combining open source information with clandestinely acquired intelligence can help paint a much clearer picture of the world than either open source or clandestinely acquired information could alone.

Moreover, open-source information can offer its own valuable intelligence insights. Take, for example, ISIL's use of social media. As I'm sure you are all aware, ISIL is a prolific, and quite proficient, user of social media. While this allows ISIL to spread its malevolent propaganda and reach out to potential recruits, it also provides us with useful intelligence.

Satellite imagery showing ISIL members gathered in a city square, for example, may not provide insight into the group's plans and intentions. But ISIL's tweets and other social media messages publicizing their activities often produce information that, especially in the aggregate, provides real intelligence value. The DDI will oversee CIA's open-source collection efforts to ensure that we make full use of this rich data set.

Regarding analysis, the DDI also will enhance the work of our analysts.

In an organization that was once heavily stove-piped, with components jealously guarding their "proprietary" information, the DDI will champion the idea that "all data is Agency data." Through both policy and technology, the new Directorate will facilitate analysts' access to information so that their products are as well-informed as

possible, while keeping information off-limits from those without a legitimate need to access it.

The DDI will also help inform analysis by developing and deploying sophisticated IT tools that will help our analysts conduct research by revealing potential linkages between and among data in our holdings. One of the real challenges of modern intelligence analysis is the sheer volume of information that is collected by our intelligence community. No one could possibly read all the intelligence reports that come in on a daily basis, and running simply Boolean word searches is not a terribly efficient or reliable way for an analyst to discover the most timely, relevant and probative intelligence.

To help solve this problem, the DDI also will be responsible for the Agency's cadre of data scientists. Housed in our new mission centers, these DDI data scientists will develop and deploy customized IT tools to help our analysts make connections in the data and test the analytic calls they make. Given the variety, complexity and volume of data we take in, this calls for some of the most sophisticated and cutting-edge programming and "big data" analysis being performed anywhere today.

Finally, the DDI will rapidly identify, transition, and deploy the best digital technologies from the private sector to bolster CIA mission execution in all areas. Building on our experience with In-Q-Tel, the highly successful technology incubator CIA established about 15 years ago, the DDI will expand our direct outreach to commercial digital entities through the establishment of a DDI business portal in Silicon Valley. This team's mission will be to identify cutting-edge technology that the Agency could use in its highly secure environment, and accelerate the integration of these solutions across our missions.

Multiple elements of the Agency in the past have responded to the challenges of the digital era. But if we are to operate as effectively as possible in the digital world, we must place our activities and operations in the digital domain at the very center of everything we do. That's the DDI's mission in the CIA of the future.

Enhancing Diversity and Inclusion

Finally, I'd like to say just a few words on what is unquestionably the most critical component of the CIA of the future—ensuring that the intelligence professionals who make up the Agency reflect the vast ethnic, cultural, educational, religious, and social diversity of this nation.

Recruiting, building and nurturing a diverse workforce at CIA is absolutely core to our mission and our modernization effort. Simply put, we are deeply committed to ensuring that the CIA of the future will more closely resemble both the world we study and the multicultural nation we serve.

On the most basic level, diversity matters to us because it is rooted in our country's fundamental belief in equality of opportunity. Because the CIA helps protect the

security of every American, every American, quite simply, deserves a full and equal opportunity to be join in this remarkable enterprise.

So quite apart from the strong business case for diversity—which I will turn to in a moment—fostering a diverse workforce is core to our mission because it is the right thing to do. We can hardly claim the mantle of being America's premier intelligence agency if we don't build and maintain a workforce as diverse as the nation we serve.

But, as I noted, diversity is also a mission imperative for CIA. Indeed, it is hard to imagine an institution that stands to benefit more from a diverse workforce than the CIA. For a number of reasons, employing intelligence professionals from all walks of life is critical to performing our work.

First, we obviously need officers who are comfortable operating in foreign environments—people with the language skills and the cultural sensitivity to mingle easily in societies that may be quite unlike our own. The more diverse our workforce, the more likely we will have the officers with these skills and qualities.

Equally importantly, we need a workforce that can bring to bear a range of perspectives on the challenges we face—and that means having officers from an array of backgrounds.

We will never develop the nuanced, comprehensive and accurate understanding of the world that our mission requires if we all think the same way. In fact, critical insights in intelligence work often come from an officer who looks at the same information as everyone else, but from a slightly different perspective, and then draws a different, and more reliable, conclusion. Diversity is key to making those insights possible.

Let me give you an example of why diversity at CIA is not just a "nice to have"—it's a necessity.

The Director and I recently met with the head of a foreign liaison service. Let's just say he was from a country where the relationship would be described as "cold." The CIA officer interpreting was a native from our visitor's country, and the language she was hearing was her mother tongue. Moreover, she had spent years in the Agency working on issues related to our visitor's country—studying the gentleman whose words she was interpreting. I can assure you, her presence, and her ability to pick up on the cultural innuendo and the nuance of language, provided the Director and me exceptional insights.

So what we need, in short, is a workforce as diverse as the world we cover.

Now this is not an especially novel insight. When our World War II forerunner, the Office of Strategic Services, was shutting down in September 1945, its chief, "Wild Bill" Donovan, remarked on the diversity of his workforce:

"We have come to the end of an unusual experiment. That experiment was to determine whether a group of Americans—constituting a cross section of racial origins, of abilities, of temperaments, and of talents—could meet and risk an encounter with long-established and well-trained enemy organizations."

The OSS, including its "experiment" in diversity, succeeded brilliantly in helping to bring victory to the Allied cause.

Yet we have to be honest: Despite the example set by our predecessor, the CIA has not always fielded a particularly diverse workforce. Indeed, the stereotypical Agency officer was a white, straight, Protestant male who drank Scotch, smoked cigarettes and graduated from an Ivy League college. That is, of course, a gross caricature—the Agency has long been comprised of a much more diverse workforce than that—but it nonetheless has some basis in reality.

Indeed, that was the unequivocal message of two recent internal studies on diversity in our leadership ranks, one led by Vernon Jordan, the other by former Secretary of State Madeleine Albright.

The study overseen by Mr. Jordan highlighted data showing that the higher the grade level at CIA, the less diversity there is in terms of race, ethnicity, and sexual orientation. The lack of diversity is particularly acute at our highest ranks, the Senior Intelligence Service, where only about one-in-ten of our officers is a minority.

Likewise, the study conducted two years ago by Secretary Albright examined why more women were not achieving promotions and positions of greater responsibility at the Agency.

Both studies offered recommendations to improve the situation, and we are in the process of implementing those recommendations, which include evaluating all our senior officers, as part of their annual performance review, on their actions to create and maintain a diverse and inclusive work environment.

But just as importantly, the entire senior leadership team—from Director Brennan on down—has made an enhanced commitment to diversity and inclusion a cornerstone of our modernization effort. This is reflected in another key element of our Modernization Program—the new Talent Center of Excellence.

This new Center is a sort of human resources operation on steroids. It is responsible for the Agency's overall efforts to recruit, train, develop and deploy our workforce. A key part of the Talent Center's mission will be to build diversity throughout the Agency, not only by strengthening our minority recruitment efforts, but by improving the way we train, manage, and develop our officers. This Center is a major investment in our people, and although its benefits may not be immediate, we expect them to be substantial over the long run.

In the end, we know this comes down to leadership—to setting the tone at the top, and to following through on the initiatives we have committed to pursue. And I can assure you, Director Brennan and I, along with the entire senior leadership team at the CIA, will do what it takes to create a more diverse and more inclusive CIA of the future, both because it is the right thing to do, and because we know that a more diverse workforce means that we will be that much more successful in producing the intelligence that our policymakers need to meet the most urgent foreign policy and national security challenges of today and tomorrow.

Conclusion

When I left Cornell 30 years ago to head off to law school, I put behind me—at least for the time-being—my interest in a career in national security. But my interest in the field, first sparked on this campus, never really faded, nor did the key lessons I learned here: work hard, ask the difficult questions, think creatively, surround myself with smart people, and make the most of my opportunities.

Today, I have the extraordinary opportunity to help lead an Agency that is, truly, central to our national security, and to address issues very much like the ones I studied here at Cornell. And what's more, I have the opportunity, working with Director Brennan and the entire leadership team at the CIA, to set the foundation for the CIA of the future—one in which an even more diverse workforce, immersed in the latest digital technology, collects and produces even better intelligence for our nation's leaders.

As a proud Cornellian, I feel both deeply privileged and perfectly well-prepared to be part of that endeavor.

Thank you.