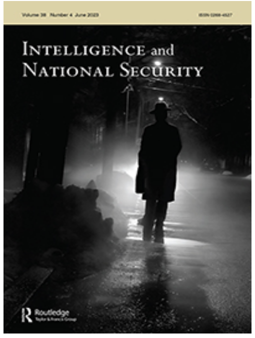

Intelligence and National Security

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/fint20

Cyber-enabled tradecraft and contemporary espionage: assessing the implications of the tradecraft paradox on agent recruitment in Russia and China

Kyle S. Cunliffe

INTELLIGENCE AND NATIONAL SECURITY
https://doi.org/10.1080/02684527.2023.2216035

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

Cyber-enabled tradecraft and contemporary espionage: assessing the implications of the tradecraft paradox on agent recruitment in Russia and China

Kyle S. Cunliffe

ABSTRACT

The acquisition of clandestine human sources – or agents – inside Russia and China likely remains the key priority for Western HUMINT agencies, and yet their ability to do this safely is quickly waning. This paper considers the utility of cyberspace for espionage recruitment in these two hard target states, and assesses its value as a potential solution to emerging surveillance threats. With the aid of history, this paper proposes that hard target espionage is fundamentally afflicted by a tradecraft paradox, one that will severely curtail the utility of cyberspace to agent recruitment.

ARTICLE HISTORY
Received 7 Sep 2022
Accepted 15 May 2023

Introduction

Espionage, or what is more often known as human intelligence, is fundamentally about people, yet this paper 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 seem 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. 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.[2] In the past, the perils of street surveillance, meaning the physical observation of foreign intelligence officers, led to new innovations in 'tradecraft', the methods used to recruit and handle spies.[3] 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. This paper is thus a study of cyber-enabled tradecraft, as a solution to a problem that intelligence officers cannot easily resolve.

Tradecraft is often regarded as more of an art than a science, 'a combination of common sense and imagination'.[4] The CIA even recruited magician, John Mulholland, to write operational manuals using established theories of deception.[5] But common sense and imagination are not enough to overcome the challenges of hard target states, meaning intelligence officers must make informed decisions about the tools and technologies to apply to their work. This was exemplified in the Cold War, where the seemingly impenetrable city of Moscow forced intelligence officers to rethink the tried and tested tradecraft of the past.[6] It kickstarted a cultural transformation, whereby for the first time in history, technology's role in espionage shifted from a minor aid to a vital function in operational affairs.[7] But despite being armed with a repertoire of tools, from cutting-edge listening devices to million-dollar spy cameras built in the garages of Swiss watchmakers, neither the CIA nor SIS ever reclaimed any significant advantage over the Soviet KGB.[8] Only a handful of agents, mainly volunteers such as Oleg Penkovsky and Adolf Tolkachev, were successfully operated within the

CONTACT Kyle S. Cunliffe ✉ k.s.cunliffe@salford.ac.uk

confines of Moscow, while others, including Oleg Gordievsky, were merely kept 'on ice' (meaning operational acts were avoided) whenever they returned to the capital.[9] This brief history lesson is important, because as the US and its allies enter what pundits are calling the 'New Cold War', with Russia and China at the very peak of national security concerns, today's practitioners face a new hard target problem.[10]

The invasion of Ukraine and rising tensions over Taiwan, echo the fact that the West has entered a new age of nation-state rivalry, one in which intelligence must be at the forefront of an effective defence. But while technical intelligence remains a key form of collection, when it comes to discerning Russia and China's most guarded secrets, including the plans and intentions of Putin and Xi, a clandestine human source – an agent, or spy – is required.[11] The problem, is that in seeking to recruit and handle those spies, intelligence officers must grapple with a new era of 'Moscow and Beijing Rules'.[12] The original Moscow Rules, derived from the Cold War, denoted conditions in which peacetime operations were beleaguered by the ever present threat of the KGB's street surveillance, to the extent that personal meetings were largely prohibited.[13] Today, aided by new developments including biometric checkpoints and smart CCTV, burgeoning and increasingly hostile armies of watchers tasked by Russia's Federal security Service (FSB) and China's Ministry of State Security (MSS) are able to identify undercover operatives and observe their movements with unparalleled speed and precision.[14] In turn, while espionage is fundamentally about people, meetings between intelligence officers and foreign officials inside Moscow and Beijing are once again becoming a prohibitively dangerous act.[15]

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*'.[16] Practitioners argue that by harnessing the benefits of cyberspace, new tradecraft can be developed to reduce or even eliminate, the need for personal meetings. Former CIA officer, David Gioe – who sees cyberspace as carrying profound revisions to tradecraft – makes a strong case that meetings will almost always have some role to play in espionage, because they offer an unrivalled means for intelligence officers to assess their agents.[17] But, if cyber-enabled tradecraft can reduce dependency on face-to-face encounters to the minimum (perhaps even to a single meeting per case), it could shift the advantage in the intelligence officers' favour. The CIA and SIS are already spending huge sums to modernise their methods, as exemplified in 2015 when the CIA revealed its first new directorate in over fifty years, *The Directorate of Digital Innovation*, for the purpose of researching and identifying technological threats and opportunities.[18] This is not an encroachment on the turf of NSA, but rather an effort to harness digital and cyber 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 it'.[19]

That being said, even if cyberspace is a powerful aid to espionage in most contexts, its utility when turned against authoritarian regimes is open to doubt. It must be considered that Russia and China are counterintelligence states, who will seek to undermine whatever advantages cyberspace affords to their opponents.[20] And if cyberspace cannot aid in the penetration of Moscow and Beijing, intelligence officers may be forced to follow in the footsteps of their Cold War predecessors, by pursuing the bulk of their sources on safer soil. In the last century, the challenges encountered in Moscow forced intelligence officers to pursue their quarry outside of the Eastern Bloc, detrimentally reducing access to the Kremlin's most senior ranks.[21] Today, Russian and Chinese officials – especially those in Putin and Xi's inner circle – are largely prohibited from travelling abroad, shifting the focus onto Moscow and Beijing.[22] Therefore, this paper assesses the value of cyberspace in recruiting agents with high level placement and access who reside in Russia and China, to determine whether it offers US and UK intelligence officers the advantage they require to pierce these hard target states. This focus on agent recruitment, rather than handling, is due to the fact it is often the most difficult stage of espionage, not least because there is no pre-existing trust between the intelligence officer and the person they aim to recruit.

It bears note that contemporary tradecraft remains one of the more opaque areas of intelligence scholarship. However, while practitioners are unlikely to be forthcoming about their knowledge of cyber affairs, the control and exploitation of cyberspace within Russia and China have been subjects of growing journalistic and academic interest. Meaning the research challenge is not in acquiring new data, but in making sense of the data that already exists. As such, owing to recent declassifications and a growing body of literature documenting the tradecraft challenges of the time, there is no period more fitting for deriving lessons that can aid this study than the West's efforts to penetrate Soviet Moscow. In turn, this paper will show that an increasing need for trust constrains the application of tradecraft in hard target conditions. Specifically, this paper hypothesizes that:

- Justifying the risks of tradecraft in hard target conditions requires greater trust in the prospective spy. However, in such conditions, the odds of failure are vastly increased since, without alternative tradecraft at their disposal, intelligence officers have few means to develop that trust.

The crux of this argument rests on the premise that any risks inherent in tradecraft increase the odds of an operational failure or, worse, increase the probability that the candidate for recruitment is a counterintelligence 'dangle' sent to waste intelligence officers' time and resources or lure them into a provocation. As these risks increase, so too does the need to justify operational acts by gathering supplementary assessment information, allowing varying degrees of trust to be developed in the prospective recruitment candidate. The problem, is that there are no clear solutions to acquiring that information without access to secure tradecraft, leading to a paradoxical situation that goes some way to explaining why high risk operational acts can be justified in some situations (e.g., where trust has been built) but not others. Herein, just as it hindered the recruitment of spies in the Cold War, this paper aims to show that through a catalogue of mounting risks and a rising need for trust, the tradecraft paradox looks set to hinder agent recruitment in the cyber era.

Spotting and assessment

Unless a source volunteers their own services, all espionage begins with the gathering of spotting and assessment data, to determine who has access to the secrets sought, what might motivate them to consider a career as a spy, and whether they are ultimately suited for clandestine work. During the Cold War, contacts and agents provided some of this data, often by supplying classified phone books containing lists of government employees.[23] Further information would be learned through interactions with foreign officials, or from operatives discretely following their targets to observe their daily habits.[24] The most intrusive insights into a person's private affairs, however, were often learned through bugging, better known as technical or audio surveillance.[25] As Easter argues, the planting of hidden listening devices in the embassies and residences of foreign officials revealed a person's 'weaknesses', 'exposing unhappy marriages, homosexual inclinations, money problems, or doubts about their own government', offering access to a plethora of deeply personal information that could aid in discerning a target's value and motive.[26]

Despite its usefulness, planting a listening device was often a hazardous undertaking, especially in hard target conditions. During most of the Cold War, bugging operations typically required lengthy installation periods, foreknowledge of the premises targeted, and a human asset to alert operatives whenever the occupant vacated the building (or to plant the bug themselves), all of which needed to be repeated whenever installed devices were detected and neutralised by 'sweeping' equipment deployed by opposing security personnel.[27] In fact, the KGB would even go so far as redecorating the residences of its foreign officials, 'baffling the effectiveness of any bugs that may have been installed'.[28] Only when technological advances enabled so-called 'quick-plant' operations in the later years of the Cold War (meaning a hidden listening device could be placed by single individual in a short amount of time), were bugging operations permitted inside Moscow, albeit even these did not eliminate the unpredictable risks of surreptitiously entering a foreign official's apartment or workplace.[29]

Any mistake in the bugging process could have exposed the recruitment target to counterintelligence, but if the bug was found, security personnel might have kept it in place, utilising the device for deceptive purposes such as seeding a dangle.[30] Gordievsky, for example, who knew his Copenhagen embassy was likely bugged by Danish intelligence, telephoned his wife to complain about the Soviet invasion of Czechoslovakia, sending his 'first, deliberate signal to the West', in an act that could just as feasibly have been used by the trained KGB officer to lure operatives into a provocation.[31] This leads into the first observation of the tradecraft paradox in action, as justifying a hazardous bugging operation required some degree of trust in a target's prospective value, as well as their likelihood of revealing information that would facilitate their recruitment.[32] Indeed, bugging was not guaranteed to reap rewards, not least because Eastern Bloc officials, who were primarily concerned with being subjected to technical surveillance by their own security services, often acted with high a degree of discretion, which somewhat helps to explain why, throughout the era, only a fraction of the CIA's bugging operations returned meaningful results.[33] As former CIA officer, Henry Crumpton, concluded after his high risk, six-month, bugging operation achieved zero results, in future missions he would gather assessment information to better understand his target.[34] 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'.[35]

Cyberspace, however, has opened up the prospect of gathering spotting and assessment data from a distance, without the hazards of a surreptitious entry. As Gioe argues, '[it] is not hyperbole to acknowledge that the twin cyber giants of social media and malicious hacking have revolutionized the ways in which intelligence services seek, locate, assess, and vet their quarry'.[36] But while it is true that by perusing spaces such as Facebook and LinkedIn, personal details can be gleaned that might otherwise have taken 'weeks or even months of personal meetings to elicit', Gioe adds that governments often regulate what their employees share online, as underscored by Britain's 'Think before you share' campaign.[37] Similar, if not stricter, measures should be expected in Russia and China; the Kremlin, for example, has banned servicemen from using smartphones (or other devices), posting photos online, or writing about the military while on duty, with culprits facing a two week jail sentence.[38] In that sense, Russia put its soldiers on similar footing to its security services, whose officers were already banned from posting about themselves or their work online (although it is worth bearing in mind that, as demonstrated throughout the war in Ukraine and the numerous leaks from within Russia via social media platforms such as Telegram, this rule appears to be frequently broken, at least by junior ranking military personnel who seem oblivious to, or undeterred by, the consequences).[39]

By contrast, the hacking of databases and personal devices offers a pathway to information that a person would not otherwise wish to share. Gioe underscores this point through the 2014 US Office of Personnel Management hack, a largescale breach by Chinese intelligence which 'lay bare 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'.[40] The value of the OPM hack to Chinese intelligence was echoed by the former US counterintelligence chief, Michelle Van Cleave:

> 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'.[41]

While the OPM hack was a devastating blow for the US, it was also indicative of the type of rewards database hacking can afford to any actor, including for the CIA's efforts to gather personal information about Russian or Chinese employees. As acknowledged by the former Director of National Intelligence, James 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'.[42] Equally tempting databases exist in the private sector, where companies sometimes place profits ahead of security; here, recruiters might find all manner of useful information, ranging from financial data to more scandalous revelations. When the dating website tailored specifically for adulterers, known as Ashley Madison, was hacked in 2013, British intelligence trawled the disclosed files to identify potential sources, as well as to ensure that their own people had not been compromised.[43]

That being said, largescale breaches are a growing concern for governments around the world, including Russia and China. Since 2015, the Kremlin has directed its scientific resources (and a small army of coerced hackers) toward strengthening national networks and databases.[44] It has also forced improvements in the private sector, by enacting strict legislation such as changing the state's definition of critical infrastructure to include healthcare, communication, banking, energy, transport and other strategically valuable sectors.[45] This means, as Sergey 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'.[46] Every company affected is obliged to bolster its cyber defences and report all detected intrusions to the government. And any company that uses insecure foreign software has been warned, by Putin himself, that they will be banned from working with government agencies.[47]

Similar steps have been taken in China, which has expanded the umbrella of critical infrastructure to include a vast swathe of companies who manage Chinese citizens' personal information, thus giving the government greater leverage to improve its cyber defences across the board.[48] Despite these measures, there has been a boom in personal information being sold on black markets in Russia and China, indicating that both governments are struggling to fully protect their citizens data.[49] One case from 2022, revealed that around one billion Chinese citizens were compromised in a database breach of the Shanghai National Police, containing criminals records pertaining to cases such as fraud and sexual assault.[50] On the one hand, the sheer scale of the breach underscores that even a regime as rich as China cannot protect all government systems from abuse (although it is worth noting that the system was not hacked; rather, a backdoor had been left open that allowed anyone to access the database if they knew where to look).[51] On the other hand, incidents of this kind are likely to encourage even greater efforts to protect critical networks, with President Xi immediately calling for public bodies to 'defend information security . . . to protect personal information, privacy and confidential corporate information'.[52]

The strengthening of defences inevitably raises the cost and time involved in committing a largescale breach, but, at a time when Western states are keen to dissuade their competitors from hacking their own systems, political implications must also be considered. 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 government indicted four Chinese hackers for similar charges, implying that Beijing is willing to use evidence of hacking for political leverage.[53] Moreover, there is always a risk that a breach may incur some form of retaliation. Obama's administration instructed the NSA to hack Russian networks in response to the 2016 DNC breach, and some US politicians called for a similar response to China over OPM.[54] As such, there exists the possibility that Russia and China will retaliate in kind to a significant breach, regardless of the intention behind the intrusion. That will not deter intelligence agencies from largescale database hacking altogether, but the potential for political fallout cannot be overlooked.

By comparison, the risks of political fallout are substantially reduced if personal information is acquired by hacking individuals, rather than databases. In 2017, a batch of documents released by WikiLeaks, called Vault 7, showed that Langley had developed a catalogue of tools for hacking popular smartphones and other personal devices.[55] Some of these hacking tools could bypass the encryption of popular instant messengers, including WhatsApp, Telegram, and Signal, lifting the cleartext logs from a target's phone.[56] Langley could even siphon a smartphone's audio, video, and geo-locational data without alerting the device's operator.[57] The prospect of turning a recruitment 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'.[58] And as more people connect 'smart' devices into their home networks, through the widening 'Internet of Things', the potential for this type of personalized hacking continues to grow. WikiLeaks, as a case in point, revealed a range of CIA hacking toolkits aimed at everything from smart televisions to smart cars.[59] One of these toolkits, 'Weeping Angel', targeted Samsung televisions, allowing access to their embedded microphones while harvesting Wi-Fi details and passwords to facilitate further penetration of the home network.[60]

Still, hacking individuals is not without risks. While Langley's hacking tools have inevitably evolved over time, the Vault 7 leaks revealed that the CIA's hacking capabilities were heavily dependent on 'zero day' exploits.[61] Zero day exploits are considered one of the most powerful tools in a hacker's arsenal, because they utilize flaws in code which are unknown to 'software makers and to the antivirus vendors'.[62] And since nobody knows that the flaw in the code exists, it is much harder to detect or block hackers who utilise them. The downside for intelligence agencies is that zero-day exploits are highly sought after by the defending side.[63] This is especially true for popular consumer brands, with mainstream companies willing to pay enormous fees (including six figure sums) for any uncovered flaws in their code.[64] Hence, in a lucrative market, the most sought after zero days are likely to be more difficult to discover while yielding shorter lifespans, making personal devices harder to hack and significantly increasing the time and resources required to do so. Indeed, both Apple and Google were quick to reassure their customers that the zero day exploits disclosed in the Vault 7 files were patched years before the leak.[65]

This challenge, along with increasingly prevalent training and awareness programmes designed to educate employees on the need to update security software as well as in how to avoid typical hacking tactics such as phishing, can render many expensive toolkits obsolete.[66] This helps explain why the Vault 7 files revealed that the CIA often required physical access to the devices they were trying to hack, to the extent that they set up a specialised 'Physical Access Group'.[67] The point about physical access is important, because, from a technical perspective, it is often easier to infect a device physically (e.g., plugging a thumb drive into a target's computer) than it is to brute force hack or 'phish' a target. In select cases, it seems that Langley managed to physically infect some devices with relatively low levels of risk. According to reports, some 'factory fresh' devices were infected by 'interdicting mail orders and other shipments … leaving the United States or otherwise', while one document suggested gifting an infected 'MacBook Air' to a target.[68]

But if gifting or interdicting a device is not possible, the obstacle of gaining physical access to a target's devices is not an easy one to resolve. Security specialist Sean Sullivan, suggests that the CIA might infect somebody's phone as they pass through airport security, while even wider promise was underscored through a GCHQ programme called 'Royal Concierge' (as revealed in the Snowden files), which intercepted booking emails from over 350 international upscale hotels.[69] Royal Concierge became an 'enabler' for espionage, allowing intelligence officers to arrive on the ground ready to meet arriving guests, and even created opportunities to bug their rooms and infect their devices.[70] However, when it comes to physically infecting the devices of Moscow and Beijing residents, intelligence officers might have little recourse other than to enter a target's home or workplace, raising similar challenges to planting a traditional hidden listening device.

Still, the level of risk and cost entailed in hacking a target's devices depends, to an extent, on whether that person (or organisation) is sensible enough to adopt best-practice security measures. In this respect, no one, not even officials in Russia and China's highest levels of state, are fully immune to the fallibility of human error, which may open up hacking opportunities. In 2019, various members of Russia's political and business elite were exposed in a cache of hacked documents known as the 'Dark Side of the Kremlin'.[71] Over one hundred gigabytes of data were released, including the personal communication logs of arms dealers, oligarchs, defence personnel, and Kremlin officials. The leaks prove that even Russia's elite are vulnerable to the consequences of incompetence, and according to *Meduza*, in some instances, 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's encrypted RSNet email system.[72] Still, proper training and disciplinary actions, which, in the current climate, are likely to be encouraged, can address many of these incompetencies, pushing hacking operations toward more challenging avenues of access and exploitation.

Especially if physical access to the target device is necessary for a breach to succeed, the above factors increase the likelihood of counterintelligence discovering a hacking operation before it reaches fruition. If counterintelligence detects a breach, they might opt for an immediate shut down, removing any malware but not before learning from its technical signatures to prevent reoccurrence. However, in some cases it may be advantageous for security personnel to allow the breach to continue, to better understand the opposing side's targets and interests, and to use that information against them. As Althoff argues, the Internet can be used to 'ferret out opponents by posing as sympathisers to their cause', and while he refers specifically to social media, the planting of fraudulent information on networks and devices is an increasingly common tactic in the defence against hackers.[73] Following a tip-off from the NSA, Emmanuel Macron's campaign team created a string of fake emails and fake information, designed to lure (and waste the time of) hackers during a significant breach in 2017, a tactic that if adopted by Russia and China, could be just as feasibly used to lure, as well deter, foreign intelligence officers.[74] Hence, given the likelihood of a breach being discovered, operatives cannot rule out the possibility that what they concurrently see or hear may be designed to attract their attention and seed a dangle.

In light of these concerns, today's intelligence officers, like their predecessors, will be better served by ascertaining whether hacking will yield actionable results, to better justify the risks that such a high risk operational act affords. Meaning, in addition to knowing the value of their target, they will want some degree of preliminary trust in the target's tendency towards indiscretion. According to 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.[75] Judah claims that these type of measures are common among Russia's elite, many of whom are fearful of being targeted in the next 'wave of sackings, arrests or even purges'.[76] Those 'privy to sensitive information no longer carry smartphones', and instead resort to 'simple old cell phones and now remove the battery – to make sure the phone is dead – when they talk about Kremlin politics among themselves', steps allegedly taken out of fear that the FSB might be eavesdropping.[77] Measures of this kind, which are likely to be echoed by China's own increasingly fearful political elite, reflect the fact that a hacking operation, even if undiscovered by counterintelligence, is hardly guaranteed to provide information that operatives can leverage for recruitment, an outcome that must call into question the wisdom of running such an operation in the first place.[78] Thus, it is arguably difficult to justify a high risk hacking operation in Moscow and Beijing conditions without , at minimum, a degree of confidence in the target's tendency to overshare, particularly in the presence of their devices.

Cultivation and five-minute pitches

Upon identifying an ideal target, the next stage (unless they volunteer) is to convince that person to become a spy. There are two approaches to recruiting an agent; one approach is to cultivate close trusting bonds with a candidate (known as a 'developmental') before a pitch – 'would you be willing to work for the CIA?' – is delivered, while the other approach is to circumvent this process altogether by delivering a pitch without any prior cultivation (known as a 'five minute pitch').[79] Throughout the Cold War, pursuing either of these approaches without revealing the recruiter's intelligence affiliations proved challenging, with contact relying primarily on personal meetings supplemented, on occasion, by secure telephone conversations. As revealed in the accounts of former CIA officer, Richard Holm, it was not abnormal for intelligence officers to initiate contact by phone, the distance of which reduced any immediate risks to the operative, before a pitch was delivered face-to-face so as to better assess and mitigate the target's reaction.[80]

Leveraging the telephone in this way was far more challenging in Moscow, due to widespread telephonic eavesdropping throughout the Soviet Union. Accounting for the extraordinary hazards of meeting a boding source, all telephone lines 'into the offices and apartments of foreigners were tapped and monitored around the clock by a virtual army of eavesdroppers'.[81] Intelligence officers could get around this problem by losing their surveillance tails and calling from payphones, but if they were observed by the KGB using public phone booths, their calls may have been traced.[82] All payphones in Moscow 'were numbered', meaning the KGB 'could easily ask for an immediate trace' of any phone call made from a specific booth.[83] Further complicating matters, should they have reached a public phone without being spotted, operatives still had to account for the fact that the telephones belonging to 'any Soviet citizen in a sensitive position' were sometimes monitored by the KGB, upping the odds of exposure.[84]

Even outside of Moscow, the workplace and apartment telephones of Eastern Bloc officials were routinely monitored by their own security services, pushing up the risks of a call's interception and, as a result of that compromise, of the target falling under counterintelligence control.[85] When attempting to recruit a Polish consulate worker, dubbed Adamski, in Turkey, the former CIA officer Duane Clarridge remained concerned about his target's proclivity for telephoning his apartment. He noted that 'hostile coverage of our meeting could already be in place if Adamski were a double agent, or if he had been careless or naïve enough to call from a phone monitored by his security personnel'.[86] This leads to the second observation of the tradecraft paradox in action, as while in Clarridge's case, the use of the telephone was out of his control, it was generally wise to develop a degree of trust in whether a candidate was worth pursuing, and likely to respond positively to a pitch, before injecting further risks. This point was all the more acute for shorter recruitment attempts, as without the development of close interpersonal bonds, a pitch was more likely to be rejected; as noted by former KGB officer, Victor Cherkashin, five minute pitches placed `great psychological pressure on a target, and often failed'.[87] Hence, as Wallace et al argue, '[operational] circumstances determined whether an individual was the subject of extended development or a cold pitch, but in either case, the assessment conducted before the question was asked loaded the dice in favor of the case officer'.[88]

But while today, meetings or telephone calls (even by smartphone or burner phone) retain many of their traditional insecurities, online social communications are seen to have opened pathways to cultivate sources without, as Wallace argues, 'revealing the hand of an intelligence service'.[89] The security of online social communications, which by nature are not covert, rests partly on the premise that cyberspace is drowning in data, meaning incriminating communications are less likely to be noticed by the opposing side's Internet surveillance. This much was illustrated, ironically, by Edward Snowden, the NSA leaker who released thousands of documents about mass surveillance. As Omand notes, Snowden's disclosures indicate that the NSA, with its enormous resources, was only capable of looking at '0.00004 per cent of the world's traffic in conducting their mission', inferring that even one of the most competent and heavily resourced technical intelligence agencies in the world, struggled to monitor the sheer volume of communications sent and intercepted via the Internet.[90] Moreover, an increasing number of social communications utilise end-to-end encryption, meaning messages can only be read by the sender and receiver. WhatsApp, for example, encrypts the messages of over a billion users to a standard that continues to frustrate intelligence and security agencies around the world.[91]

These factors have certainly worked to the advantage of the West's competitors. In 2017, the German federal security service, the BfV, accused China of targeting over 10,000 German citizens through 'networks like LinkedIn'.[92] As *Newsweek* reported, Chinese intelligence officers posed as 'academics, business consultants and policy experts' to cultivate relations with 'high profile politicians and business leaders'.[93] Yet the BfV struggled to counter China's activities on LinkedIn, because it had little way to differentiate between the communications of Chinese intelligence officers and those of ordinary LinkedIn users, as the agency acknowledged, '[the] infections are difficult to detect, since network connections between service providers and their customers aren't suspicious. This gives the attack an even better disguise than before'.[94] However, one report released by Snowden, shows that Western intelligence officers, in the right conditions, are equally prepared to cultivate targets online. Written for GCHQ's *Joint Threat Intelligence Group* (JTRIG), the report reveals how GCHQ uses cyberspace to conduct a wide variety of missions.[95] Most of these missions appear to be focused on influencing behaviours rather than espionage, but JTRIG occasionally tried 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 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.[96]

In short, GCHQ conducts the groundwork, cultivating online relationships in forums and social networks, before passing the reigns to SIS for the target to be further developed. In theory, any online social medium could be utilised for agent cultivation. Snowden's files, for example, revealed that various agencies, including the FBI and CIA, ran 'HUMINT operations' inside 'massively multi-player' online video games, to the extent that they even considered establishing a 'deconfliction and tipping group' to avoid overlap and improve collaboration.[97] Another leaked memo, produced by GCHQ and read by *The Guardian*, claimed that World of Warcraft, a massively multiplayer online game with several million players, contained a rich list of targets, including 'telecom engineers, embassy drivers, scientists, the military and other intelligence agencies'.[98]

But the outlook of online cultivation must be weighed against the fact that Russia and China continue to expand surveillance of the Internet, ironically through laws designed to protect their citizens from Western Internet surveillance.[99] China is well known for its tight control of the Internet, having blocked its citizens from accessing foreign services such as Google and Facebook through the 'Great Firewall'.[100] Snowden's 2013 mass surveillance disclosures, however, served as the ideal excuse for Beijing to further tighten its grip over cyberspace. Since 2015, China has enacted sweeping legislation forcing companies to relocate Chinese data into the mainland, curbing US eavesdropping by ensuring that data is held in servers that cannot be accessed by Western intelligence agencies.[101] Similar measures followed in Russia, where the introduction of the 2015 Data Localization Act claimed to protect Russian citizens from the 'misuse of their personal data by foreign companies and surveillance by foreign governments'.[102] The government blocked access to LinkedIn in 2016 for refusing to relocate its servers into Russia, while further threats supposedly resulted in the compliance of at least Google and Apple.[103] It also bears note that since the invasion of Ukraine, Russia has completely blocked access to Facebook, Twitter, and Instagram, cutting off its citizens access to some of the world's most popular social platforms.[104]

Although data localization protects citizens from foreign surveillance, it also makes them more vulnerable to eavesdropping by their own governments. While surveillance of the Internet is thought to be widespread throughout China, much of which is relegated to the private sector, a similar outlook is emerging in Russia. Prior to the Localisation Act, Russian officials saw the 'uncontrolled use' of foreign services such as 'Skype, Gmail, and Hotmail' as potential challenges to state security, because their servers were located abroad where they could not be accessed by the FSB.[105] Now, any major company with servers located in Russia is compelled to install SORM black boxes, a technical eavesdropping system that feeds data, including telephone, email, and social media traffic, to FSB facilities across the country.[106] That information can be accessed at the FSB's discretion, without any need to give a warrant to the company holding the data.[107] As one FSB officer told *Wired*, they 'can use SORM to take stuff off their servers behind their backs'.[108] Russian citizens are placed on SORM watchlists for a variety of indiscretions, including attending anti-regime demonstrations or for expressing support for Putin's opponents on social media.[109] Official figures show that in a mere six years, annual SORM intercepts doubled, rising to 539,864 cases by 2012.[110] And yet, this figure could be far higher, since it does not include the number of people targeted by SORM surveillance for counterintelligence purposes.

These are not problems that can be fixed by something as simple as deleting a message, since communication logs (including content and metadata) are likely to be stored for a substantial length of time. In 2016, Russia introduced a bill better known as Yarovaya's Law, obligating companies to store communication data for six months and metadata for three years (in a move criticised for its high financial costs), vastly extending the timeframe in which an incriminating message could be uncovered.[111] And since Yarovaya's Law forces companies to provide communication data on request, it essentially outlawed end-to-end encryption applications such as WhatsApp. But despite being delegitimised, Russia has not been wholly successful in blocking encrypted messengers. The Kremlin tried to block Telegram – a Russian made encrypted messenger that is widely used by privacy activists, criminals, and the political and economic elite – in 2018, but it was unable to do so without disrupting other services including Google and Amazon.[112] Nonetheless, the Kremlin has not given up on its efforts, levelling threats at a wide range of popular applications (including WhatsApp), with one official asserting that any company who failed to comply with Yarovaya's Law 'will be blocked sooner or later'.[113] Likewise, China fully blocked access to WhatsApp in 2017, and the only remaining encrypted platform in the country – Apple messenger – remains under doubt. To date, Apple has been accused of making compromises in terms of its customers security in order to comply with China's security laws, as one experts notes, the 'Chinese are serial iPhone breakers'.[114]

These ongoing efforts demonstrate that Russia and China are fully determined to shut down or control any potential pathway to privacy in cyberspace, regardless of medium. Even video games have not gone unscathed, with China reportedly attempting to ban all interaction with foreigners in online games, due to what it perceives as a key security loophole.[115] Likewise, the widely popular online game, League of Legends, briefly suspended all voice chat functionality for its Russian players, because its developers were unable to find the capacity to store that data as dictated by Yarovaya's Law.[116] Moreover, a key part of the problem facing any Russian and Chinese citizen in cyberspace, let alone the operatives seeking to recruit them, is that it is increasingly difficult to determine what is secure and what is not. Telegram, for example, is consistently lauded as a relatively secure app in Russia, one that is used by a significant number of Russian citizens who oppose Putin.[117] However, since the war in Ukraine, there are growing numbers of reports suggesting that Telegram may have been compromised by Russian security services, but it remains unclear as to how, if it all, the Russian security services have achieved this goal.[118]

The sheer outreach of this surveillance – not to mention the risks that a target's personal devices might be monitored by their own security services – calls into question the wisdom of sustained online contact. This much was demonstrated in a case reported in Chinese state media, involving a low-level agent known as 'Li', who was recruited online by a foreign operative dubbed 'Feige'.[119] In one respect, the fact that Li (a low-ranking agent, sentenced to ten years in prison) was run for several years through China's 'QQ' messenger, suggests, as Mattis argues, that despite the government's vast surveillance powers, its security services still have 'trouble tracking the flow of information'.[120] And yet, in what should serve as a dire warning for other recruiters, it is reported that once the authorities narrowed their investigation, Feige's historic communication logs unmasked around forty additional 'suspected spies'.[121] Still, the evidence certainly suggests that, in the right circumstances, operatives are willing to use a minimal amount of online interaction to facilitate a swift recruitment, even in hard target conditions, as illustrated by the CIA's efforts to lure Iranian candidates over the border using fake online job websites.[122] Such a move is less effective against officials who cannot travel abroad freely, but a single introductory message sent to a Russian or Chinese official by a medium such as Telegram or Apple Messenger, may be sufficient to elicit enough information about a person's whereabouts and availability in order to arrange a daring meeting, without creating enough noise so as to attract the attention of Internet surveillance.

Nonetheless, doing so securely would depend on whether the target accessed their messages from a secure device (as opposed, for example, to a work computer), as well as the degree to which that person, as well as their devices, was already under scrutiny by their own security services.

Thus, today's intelligence officers face significant challenges when pitching spies, as even a seemingly innocuous online relationship can compromise a case and increase the risk of a target falling under counterintelligence control. No matter how brief, any contact stands a chance of being monitored by Internet surveillance, but when the nature of a relationship becomes more personal, or the content of the interaction raises potential red flags (such as attempts to elicit information), the risks only mount. Once alerted, counterintelligence may opt to put an end to a growing relationship, or, if a dangle operation is preferred, security personnel can take control of a person's online accounts and impersonate them, turning the operation back against the intelligence officer doing the recruiting. This was illustrated by the fate that befell one Russian operative who was duped by US security officials posing as the Russian's own recruitment target.[123] Specifically, the Russian operative attempted to pressure a US diplomatic official by email, and when the official reported the incident, 'American security officials impersonated the diplomat in a reply email and arranged their own meeting with the Russian, turning the game back on him'.[124]

In light of these issues, before initiating contact with Russian or Chinese officials in cyberspace, it is essential that today's operatives, not unlike their predecessors, justify such an operational act by developing some degree of trust in their target. Compared to a slow burning developmental, a five minute pitch would involve less contact time but also require robust assurances that the target is worth pursuing and is willing to cooperate with a proposal to engage in espionage. And yet, because counterintelligence concerns are high in these countries, any out of the ordinary online interaction may in fact add to the psychological pressures that a short recruitment affords. China, for example, runs various public awareness campaigns, forewarning its citizens, particularly those with access to sensitive or classified information, about the threat of ostensibly friendly foreigners using cyberspace to recruit spies and elicit information, cultivating a culture of awareness that potentially increases the probability of a target rejecting an intelligence officer's advances.[125] When it comes to staving off such concerns, by building trust, Grey argues that today's recruiters are armed with so much prior assessment information that a pitch can be 'accelerated' with a greater' chance of success'.[126] However, at least where hard targets are concerned, this perspective appears somewhat optimistic. If that preliminary assessment information cannot be obtained by other means (such as hacking), meaning operatives cannot develop sufficient trust before the pitch is delivered, then it is difficult to perceive how any recruitment attempt aided by cyberspace can be justified in Moscow or Beijing conditions.

Volunteers

The complications encountered in cultivation, could be skipped altogether if a source volunteers their own services. In the Cold War, volunteers in most parts of the world pitched their desire to spy by entering or telephoning foreign embassies, where they could speak directly to diplomatic officials. However, in Moscow, round-the-clock physical and technical surveillance of embassies made it difficult for people to offer their services, with the handful of known successes – Adolf Tolkachev and Oleg Penkovsky – approaching foreign nationals in the street, in the hope that someone would relay their messages to the West.[127] When an offer to volunteer was received, formulating a response presented its own challenges. Short telephone calls (made from payphones) offered more security for the officer making the response than a personal meeting, but these came at the expense of endangering the person on the receiving end.[128] For instance, while responding to Tolkachev by telephone – who was instructed to pick up a dead-drop containing secret writing equipment for further communication – posed few complications, CIA officers viewed a failed attempt to telephone Penkovsky as 'totally useless . . . dangerous and stupid'.[129]

Intelligence officers viewed volunteers in Moscow with a heightened degree of suspicion, but the inherent risks of their approach (as well as any means of response) furthered concerns about candidates falling under the scrutiny or control of counterintelligence.[130] The CIA assessed that even if Tolkachev was bona fide initially, his high risk method of approaching cars with American license plates in gas stations increased the probability of him being monitored or controlled by the KGB, leading Langley to reject initial proposals by its officers in Moscow to arrange a meeting.[131] This leads into the third observation of the tradecraft paradox in action, as in light of such concerns, justifying a response required greater trust in a candidate's existing and potential access to classified information, their suitability for spy work, as well as the motivating factors that might have driven them to take such significant risks.[132] Some volunteers established this trust as part of their initial pitch, if they were willing to share incriminating information over insecure channels. From the onset, Penkovsky provided bona fides strong enough to prompt officers into various daring attempts to respond, while Tolkachev resisted, sharing only a small amount of evidence in his early attempts to contact the CIA.[133] That finite evidence was viewed with a heightened degree of scepticism, but despite not convincing Langley to approve his immediate request for a meeting, it did justify approval for a less risky (for the intelligence officer) telephone response.[134]

But while entering or phoning foreign embassies, or even approaching foreign officials, remains a hazardous act for Moscow or Beijing residents, it is now possible for candidates to volunteer their services online.[135] Both SIS and the CIA provide online contact forms on their websites, allowing interested parties to pitch directly to intelligence agencies. According to the CIA's website, sources can use this system if they want to share information that may be useful to its foreign intelligence collection mission.[136] This method of contact proved useful in the 2009 case of Roman Ushakov, of Russia's Interior Ministry (MVD), who initiated contact through the CIA's website, becoming 'a kind of spotter' for the agency.[137] Ushakov, a low-ranking officer of Russia's Interior Ministry (MVD), offered insider access to his own agency, as well as the identities of around a dozen FSB officers. Similarly, Yevgeny Chistov, a former Russian police officer, is thought to have pitched his services online around 2011, securing a response from the CIA in ten days.[138]

And yet, approaching intelligence agencies in this way is not without its risks, since, as SIS warns, connections to intelligence agency websites are 'monitored by most governments'.[139] To an extent (and very much depending on the environment), this problem can be mitigated by taking precautionary steps, including, as SIS recommends, messaging from disposable devices or Internet cafes.[140] The CIA has even set up an online contact site in the dark web, which can be accessed using The Onion Router (Tor) for an extra layer of security.[141] But the safest online approach, according to SIS, is to 'not contact us from inside your own country, or from a country likely to share security information with your country'.[142] But even if a message is received, the feasibility of a secure response will very much depend on the technical aptitude of the person making the offer. In 2013, one CIA officer, named Ryan Fogle, was caught in Russia trying to a deliver a letter to a would-be source, which included instructions to continue contact by Gmail.[143] This may sound promising, but as Russia and China have tightened their grip over cyberspace, a response of this kind is dangerous. And while the risks can be mitigated if a person provided clear instructions for a more secure reply (such as using Tor from a disposable device), it only takes a single laps in tradecraft by either party to draw the attention of counterintelligence.

These risks likely exacerbate broader concerns about operational compromise and provocations. Regardless of whether the volunteer was bona fide initially, any attempt to contact an agency website (or respond accordingly) significantly increases the odds of counterintelligence involvement. Once again, officers must assume that if opposing security personnel were to identify the culprit, they would put an end to their efforts or take control of their online persona and run their own operation in their stead. Heightening these concerns is the ease at which Russian and Chinese security services can exploit intelligence agency websites to their advantage. In 2016, Russian media claimed that two Russian fraudsters had emailed the CIA's website offering fake military secrets, spurring on the CIA's curiosity and leading officers 'up the garden path'.[144] Incidents of this nature, some of which may be manufactured by the opposition to waste their time and resources, have somewhat soured intelligence officers' expectations of anyone contacting an agency website, as candidly put by former CIA officer, Colin Thompson, 'the CIA should view any Russian volunteer using that channel as a likely provocation or, if not, a fool who should be ignored'.[145] Until recently, the CIA even included the follow warning on its website: 'Attention: If you are a citizen of the Russian Federation, please do not contact us via this site'.[146]

In turn, it is likely that today's intelligence officers, in parallel to their Cold War counterparts, will want strong assurances about the prospective spy's placement, access, suitability and motive, before initiating a high risk response. It bears note, for example, that in the cases of Roman Ushakov and Yevgeny Chistov, both agents were reportedly able to meet with CIA officers abroad, under circumstances that allowed for a safer assessment. However, in the absence of such conveniences, and when entirely dependent upon inherently insecure means of contact, the need for a degree of preliminary trust before initiating a hazardous reply is arguably more significant.[147] Here, it is impossible to determine whether high value volunteers will be willing to share bona fides across blatantly insecure channels, since the interception of personal information could ultimately expose the would-be spy to their own security services. Of course, some volunteers will be savvy enough to securely communicate (perhaps through Tor) some degree of personally identifiable information, but that is entirely dependent on the aptitude, and willingness, of the individual in question; arguably, the high risks of a compromise through any degree of online interaction are likely to deter a growing number of cautious candidates from doing so. However, should such assessment information be unobtainable by other means, it is hard to see how operatives can develop the necessary trust to justify responding, either online or in person, to Moscow or Beijing residents pitching their services through intelligence agency websites.

The tradecraft paradox

Consequently, this paper demonstrates the recurring challenges embedded in agent recruitment. In one respect, cyberspace is a tradecraft game-changer, opening up capabilities that profoundly alter how targets are found and recruited. But in another respect, the risks inherent to cyber-enabled tradecraft are very much a continuation of the risks encountered in the past. The result, as initially hypothesised, is that *the risks of tradecraft in hard target conditions requires greater trust in the prospective spy. However, in such conditions, the odds of failure are vastly increased since, without alternative tradecraft at their disposal, intelligence officers have few means to develop that trust*. Indeed, when it comes to recruiting agents with high level placement and access in Moscow and Beijing, this tradecraft paradox seems likely to undermine whatever advantages cyberspace affords, just as it undermined the benefits of tradecraft and technology in the Cold War.

In the last century, the inability of operatives on the ground to develop sufficient trust to justify their tradecraft, left few options to recruit spies beyond the handful of high value volunteers who were willing to provide assessment information on their own initiative. In parallel, under mounting risks, tradecraft enabled by cyberspace simply cannot be justified without ensuring that those risks – including the fact that any misstep in tradecraft increases the probability that the person being pursued for recruitment is a counterintelligence dangle – are not being undertaken needlessly. This situation places today's intelligence officers in the same dilemma as their predecessor, since they cannot develop necessary assurances without recourse to secure tradecraft. Undoubtedly, the mere prospect that a person has access to valuable intelligence, even without proof, may be enough to spur some risk-taking operatives into action without developing sufficient trust to justify an operational act, but doing so would increase the odds of failure, put lives in danger, push up the probability of recruiting a dangle, and reduce operational successes to luck and intuition, none of which offers a sustainable or ethical strategy for moving forwards.

No doubt, there will be occasional exceptions – SIS officers might discover a target with poor digital hygiene and a proclivity for gossip, before hacking his devices and using that data to run a five-minute pitch arranged online, or perhaps a tradecraft-savvy officer of China's Ministry of State Security might pitch her services to the CIA's website, providing strong bona fides and instructions for a secure response. But when pitted against aggressive and heavily resourced counterintelligence, opportunities of this fashion are likely to be rare, and unless there are radical changes to cyberspace as a whole, the tradecraft paradox is unlikely to be resolved. Operatives are more likely to achieve success by recruiting the bulk of their sources on safer soil, yet doing so cuts off access to the majority of desired agents in the highest ranks of government, especially those in Putin and Xi's inner circles who are forbidden from foreign travel. That said, by pursuing agents outside the hazardous confines of Moscow and Beijing, where the tradecraft paradox offers little reprieve, intelligence officers are better able to harness the advantages that cyberspace affords. Nevertheless, without a sufficient means to develop trust, Russia and China's most guarded – and most valued – secrets are likely to remain hidden.

Notes

1. Wilder, 'The Psychology of Espionage', 19–34.
2. Gioe, '"The More Things Change"', 220.
3. Ibid.
4. Holm, *The Craft we Chose*, 275.
5. Wallace and Melton, *C.I.A. Manual of Trickery and Deception*, 15.
6. C Mendez, Mendez, and Baglio. *The Moscow Rules*, 20–21.
7. Wallace, et al, *Spycraft*, 36–40.
8. Russel, *Sharpening Strategic Intelligence*, 51–52.
9. See for example Gioe, 'Handling HERO' and Hoffman, *The Billion Dollar Spy*.
10. *National Security Strategy*, 6–9.
11. Cunliffe, 'Hard Target Espionage', 1019.
12. Ibid, 1028.
13. Mendez, Mendez, and Baglio. *The Moscow Rules*, 19–21.
14. Cunliffe, 'Hard Target Espionage', 1019–1028.
15. Ibid.
16. 'CIA-GW intelligence conference'.
17. Gioe, '"The More Things Change"', 221.
18. Cunliffe, 'Hard Target Espionage', 1025–1026.
19. *Reuters*, 'Digitizing the CIA: John Brennan's Attempt to Lead America's Spies Into the Age of Cyberwar'.
20. According to Dziak, referring to the Soviet Union, in a counterintelligence state 'the discovery and elimination of perceived conspiracies and enemies characterized the motives and behavior of an intermeshed party and state security apparat'. Dziak, 'The Soviet System of Security and Intelligence', 41.
21. Russel, *Sharpening Strategic Intelligence*, 51–52.
22. Cunliffe, 'Hard Target Espionage', 1020–1021.
23. Gioe, '"The More Things Change"', 219.
24. Wallace, et al, *Spycraft*, 367–368.
25. Ibid, 365.
26. Easter, "Soviet Bloc and Western Bugging of Opponents', 31.
27. Wallace, et al, *Spycraft*, 230; Crumpton, *The Art of Intelligence*, 67–70; Dulles, *The Craft of Intelligence*, 63–64.
28. Marchetti and Marks, *The CIA and the Cult of Intelligence*, 190.
29. Wallace, et al, *Spycraft*, 159 and 228–229.
30. Dulles, *The Craft of Intelligence*, 64.
31. Gordievsky, *Next Stop Execution*, Ch. 7.
32. Crumpton, *The Art of Intelligence*, 70.
33. Aldrich, *GCHQ*, 3; Wallace, et al, *Spycraft*, 231.
34. Crumpton, *The Art of Intelligence*, 70.
35. Ibid.
36. Gioe, '"The More Things Change"', 218.
37. Ibid.
38. Lokhov, 'How and Why the Russian Military Puts Soldiers in Jail for Using Smartphones and Social Media'.
39. *BBC News*, 'Russian Soldiers Face Ban on Selfies and Blog Posts'.
40. Gioe, 'The More Things Change', 218.
41. Van Cleave, 'Chinese Intelligence Operations and Implications for U.S. National Security', 1.

42. Pepitone, ‘China is “Leading Suspect” in OPM Hacks, Says Intelligence Chief James Clapper’.
43. Farmer, ‘British Spies Trawl Ashley Madison Leak for Intelligence’.
44. Baranovskaya, ‘Moscow’s Cyber-Defense’.
45. Sukhankin, ‘Russia on the Verge of a “Cyber Purge?”’.
46. Ibid.
47. *Reuters*, ‘Putin Tells Russia’s Tech Sector: Ditch Foreign Software or Lose Out’.
48. Yang, ‘China’s Cyber Security Law Rattles Multinationals’.
49. Feng, ‘In China, a New Call to Protect Data Privacy’.; Zakharov, ‘Russian Data Theft: Shady World Where all is for Sale’.
50. Tidy, ‘Security Warning after Sale of Stolen Chinese Data’.
51. Ibid.
52. Ibid.
53. Satter, ‘Chinese Cybersecurity Company Accuses CIA of 11-Year-Long Hacking Campaign’.
54. Miller et al, ‘Obama’s Secret Struggle to Punish Russia for Putin’s Election Assault’.; Sanger, ‘U.S. Decides to Retaliate Against China’s Hacking’.
55. *WikiLeaks*. ‘Vault 7: CIA Hacking Tools Revealed’.
56. Barrett, ‘Don’t Let WikiLeaks Scare You off of Signal and Other Encrypted Chat Apps’.
57. *WikiLeaks*. ‘Vault 7: CIA Hacking Tools Revealed’.
58. Matthew and Bodner. ‘Spy Games’.
59. Greenberg, ‘How the CIA Can Hack Your Phone, PC, and TV (Says Wikileaks)’.
60. Wikileaks, ‘Weeping Angel (Extending) Engineering Notes’.
61. Greenberg, ‘How the CIA Can Hack Your Phone, PC, and TV (Says Wikileaks)’.
62. Zetter, *Countdown to Zero Day*, 8.
63. Ibid, 110.
64. Greenberg, ‘Here’s a Spy Firm’s Price List for Secret Hacker Techniques’.
65. Burgess, ‘Wikileaks Drops “Grasshopper” Documents, Part Four of Its CIA Vault 7 Files’.
66. A good example of this is the FBI’s Know the Risk Raise Your Shield programme. For more information, see *ODNI*. ‘Know the Risk Raise Your Shield’.
67. *WikiLeaks*. ‘Vault 7: Projects’.
68. *CIA*. 2009. ‘DarkSeaSkies 1.0 User Requirements Document’.
69. *The Telegraph*. ‘British and US Spies at Risk After Wikileaks Publishes Top-secret CIA Spyware Document’.; Poitras, et al. “GCHQ Monitors Diplomats’ Hotel Bookings”.
70. Poitras, et al. “GCHQ Monitors Diplomats’ Hotel Bookings”.
71. Mackinnon, ‘Hackers Turn the Tables on Russia’.
72. Baranovskaya, ‘Moscow’s Cyber-Defense’.
73. Althoff, ‘Human intelligence’, 75.
74. Nossiter, Sanger, and Perlroth, ‘Hackers came, but the French Were Prepared’.
75. Miller, ‘As Russia Reasserts Itself, U.S. Intelligence Agencies Focus Anew on the Kremlin’.
76. Judah, ‘Putin’s Coup’.
77. Ibid.
78. *CNN*, ‘What Happened to China’s Former Leader Hu Jintao?’.
79. Wallace, et al, *Spycraft*, 364.
80. Holm, *The Craft we Chose*, 292.
81. Mendez and McConnell, *The Master of Disguise*, 221.
82. Hoffman, *The Billion Dollar Spy*, Ch. 4.
83. Ibid.
84. Mendez and McConnell, *The Master of Disguise*, 221.
85. *A Spy for all Seasons*, 139.
86. Ibid.
87. Cherkashin and Feifer, *Spy Handler*, 120.
88. Wallace, et al, *Spycraft*, 364.
89. Wallace, ‘A time for counterespionage’, 113.
90. Omand, ‘Understanding Digital Intelligence and the Norms That Might Govern It’, 3.
91. Kelion, ‘WhatsApp’s Privacy Protections Questioned After Terror Attack’.
92. Cuthbertson, ‘China Is Spying on the West Using LinkedIn, Intelligence Agency Claims’.
93. Ibid.
94. Ibid.
95. Dhami, ‘Behavioural Science Support for JTRIG’s (Join Threat Research and Intelligence Group) Effects and Online HUMINT Operations’, 9–11.
96. Ibid.
97. *NSA*, ‘Exploiting Terrorist Use of Games & Virtual Environments’.

98. Ball, ‘Xbox Live among Game Services Targeted by US and UK Spy Agencies’.
99. Sargsyan, ‘Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security’, 2225–2229.
100. Deibert, *Black Code*, 62.
101. Zhou, ‘China’s Comprehensive Counter-Terrorism Law’.; Wong, ‘China Adopts Cyber Security Law in Face of Overseas Opposition’.
102. Daniel and Byhovsky, ‘Privacy and Data Protection in Russia’, 241–242.
103. Lunden, ‘Russia Says “Nyet” Continues LinkedIn Block after It Refuses to Store Data in Russia’.
104. Bond and Allyn, ‘Russia is Restricting Social Media. Here’s What We Know’.
105. Lowenthal, *Intelligence: From Secrets to Policy*. Ch. 17.
106. Soldatov and Borogan, *The Red Web*. Ch. 8.
107. Soldatov and Borogan, ‘Russia’s Surveillance State’, 24–25.
108. Soldatov and Borogan. ‘In Ex-Soviet States, Russian Spy Tech Still Watches You’.
109. Morgus, ‘The Spread of Russia’s Digital Authoritarianism’, 90–91.
110. Soldatov and Borogan, I, ‘Russia’s surveillance state’, 25.
111. *Meduza*. ‘Russia’s State Duma just Approved some of the most Repressive Laws in Post-Soviet History’.
112. Burgess, ‘This Is Why Russia’s Attempts to Block Telegram Have Failed’.; Loucaides, ‘The Kremlin Has Entered the Chat’.
113. Sudakov, ‘Russia May Block Whatsapp, Viber, Telegram Even Tomorrow’.
114. Ibid.
115. Yang, ‘China to Ban Online Gaming, Chatting with Foreigners outside Great Firewall’.
116. Heath, ‘Riot Finally Enables Voice Chat for Russian Players in VALORANT’.
117. Loucaides, ‘The Kremlin Has Entered the Chat’.
118. Ibid.
119. Brookes, ‘Is China Swarming with Foreign Spies?’.
120. Mattis, ‘Virtual Espionage Challenges Chinese Counterintelligence’.
121. Brookes, ‘Is China Swarming with Foreign Spies?’.
122. Dorfman and McLaughlin. ‘The CIA’s Communications Suffered a Catastrophic Compromise. It Started in Iran’.
123. Matthew and Bodner. ‘Spy Games’.
124. Ibid.
125. Liao, ‘China’s Education Group Released a Cartoon Encouraging Kids to Embrace Counterespionage’.
126. Grey, S. *The New Spymasters*, 277.
127. Victor Sheymov described contacting the American embassy in Moscow as ‘out of the question’. For more details, see: Sheymov, *Tower of Secrets*, 288; Duns, *Dead Drop*, Ch. 2; Hoffman, *The Billion Dollar Spy*, Ch. 2, 3 & 4.
128. Hoffman, *The Billion Dollar Spy*, Ch. 3.
129. Ashley, *CIA SpyMaster*, Ch. 10.
130. *The Billion Dollar Spy*, Ch. 4.
131. Ibid.
132. Ibid; Duns, *Dead Drop*, Ch. 2.
133. Hoffman, *The Billion Dollar Spy*, Ch. 4.
134. Ibid.
135. Althoff, ‘Human intelligence’, 75.
136. *SIS*. ‘Sharing Information Securely’.
137. Stein, ‘The Russian Spy Who Came in through the Email’.
138. Merzlikin, ‘“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’.
139. *SIS*. ‘Sharing Information Securely’.
140. Ibid.
141. Newman, ‘The CIA Sets Up Shop on Tor, the Anonymous Internet’.
142. *SIS*. ‘Sharing Information Securely’.
143. *The Telegraph*, ‘CIA Agent “detained in Moscow”: His “letter” in Full’.
144. *Yahoo! News*. “Russia Busts Pair ‘Trying to Sell CIA Fake Secrets”.
145. Stein, ‘The Russian Spy Who Came in Through the Email’.
146. *CIA*. ‘Contact Us’.
147. Stein, ‘The Russian Spy Who Came in through the Email’.; Merzlikin, ‘“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’.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

Kyle S Cunliffe is a Lecturer in International History in the Politics and Contemporary History Faculty at the University of Salford. His PhD and wider research addresses the impact of cyberspace on espionage and counterintelligence.

References

Aldrich, R. J. *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*. London: Harper Press, 2010.

Althoff, M. "Human Intelligence." In *The Five Disciplines of Intelligence Collection*, edited by M. Lowenthal and R. M. Clark, 45–80. Thousand Oaks: CQ Press, 2016.

Ashley, C. *CIA Spymaster: Kisevalter, the Agency's Top Case Officer, Who Handled Penkovsky and Popov*. Gretna: Pelican Publishing Company, 2004.

Ball, J. "Xbox Live Among Game Services Targeted by US and UK Spy Agencies." *The Guardian*, December 9, 2013. https://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life.

Baranovskaya, S. "Moscow's Cyber-Defense: How the Russian Government Plans to Protect the Country from the Coming Cyberwar." *Meduza* (July 19, 2017). https://meduza.io/en/feature/2017/07/19//moscow-s-cyber-defense

Barrett, B. "Don't Let WikiLeaks Scare You off of Signal and Other Encrypted Chat Apps". *Wired*, March 7, 2017. https://www.wired.com/2017/03/wikileaks-cia-hack-signal-encrypted-chat-apps/.

BBC News. "Russian Soldiers Face Ban on Selfies and Blog Posts." October 5, 2017. http://www.bbc.co.uk/news/world-europe-41510592?ocid=socialflow_twitter.

Bond, S., and B. Allyn. "Russia is Restricting Social Media. Here's What We Know." *NPR*, March 21, 2022. https://www.npr.org/2022/03/07/1085025672/russia-social-media-ban.

Bradsher, K. "China Blocks WhatsApp, Broadening Online Censorship." *The New York Times*, September 25, 2017. https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html.

Brookes, A. "Is China Swarming with Foreign Spies?" *Foreign Policy*, November 4, 2014. http://foreignpolicy.com/2014/11/04/is-china-swarming-with-foreign-spies/.

Burgess, M. "This is Why Russia's Attempts to Block Telegram Have Failed." *Wired*, April 18, 2018. https://www.wired.co.uk/article/telegram-in-russia-blocked-web-app-ban-facebook-twitter-google.

Burgess, M. "WikiLeaks Drops 'Grasshopper' Documents, Part Four of Its CIA Vault 7 Files." *Wired*, May 7, 2017. https://www.wired.co.uk/article/cia-files-wikileaks-vault-7.

Cherkashin, V., and G. Feifer. *Spy Handler, Memoir of a KGB Officer*. New York: BasicBooks, 2005.

CIA. "Contact Us." July 1, 2021. https://www.cia.gov/cgi-bin/forlang_form.cgi.

CIA. 2009. "DarkSeaskies 1.0 User Requirements Document." January. Published by WikiLeaks, March, 23, 2017. https://wikileaks.org/vault7/darkmatter/document/DarkSeaSkies_1_0_URD/DarkSeaSkies_1_0_URD.pdf.

Claridge, D. R., and D. Diehl. *A Spy for All Seasons: My Life in the CIA*. New York: Scribner, 1997. Kindle.

CNN. "What Happened to China's Former Leader Hu Jintao?" October 28, 2022. https://edition.cnn.com/2022/10/28/china/china-party-congress-hu-jintao-new-video-intl-hnk/index.html.

Crumpton, H. A. *The Art of Intelligence: Lessons from a Life in the Cia's Clandestine Service*. New York: Penguin Books, 2012.

Cunliffe, K. S. "Hard Target Espionage in the Information Era: New Challenges or the Second Oldest Profession." *Intelligence & National Security* 36, no. 7 (2021): 1018–1034. doi:10.1080/02684527.2021.1947555.

Cuthbertson, A. "China is Spying on the West Using LinkedIn, Intelligence Agency Claims." *Newsweek*, December 11, 2017. http://www.newsweek.com/china-spying-west-using-linkedin-743788.

Deibert, R. J. *Black Code: Inside the Battle for Cyberspace*. Toronto: McClellend & Stewart, 2013.

Dhami, M. K. "Behavioural Science Support for Jtrig's (Join Threat Research and Intelligence Group) Effects and Online HUMINT Operations." Statewatch, June 22, 2015. 9–11, https://www.statewatch.org/media/documents/news/2015/jun/behavioural-science-support-for-jtrigs-effects.pdf.

Dorfman, Z., and J. Mclaughlin. "The Cia's Communications Suffered a Catastrophic Compromise. It Started in Iran." *Yahoo News*, November 2, 2018. https://uk.finance.yahoo.com/news/cias-communications-suffered-catastrophic-compromise-started-iran-090018710.html.

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.

Duns, J. *Dead Drop: The True Story of Oleg Penkovsky and the Cold War's Most Dangerous Operation*. London: Simon & Schuster, 2013.

Dziak, J. J. "The Soviet System of Security and Intelligence." In *Security and Intelligence in a Changing World*, edited by A. S. Farson, D. Stafford, and W. K. Wark, 25–45. New York: Routledge, 2021.

Easter, D. “Soviet Bloc and Western Bugging of opponents’ Diplomatic Premises During the Early Cold War.” *Intelligence & National Security* 31, no. 1 (2016): 28–48. doi:10.1080/02684527.2014.926745.

Farmer, B. “British Spies Trawl Ashley Madison Leak for Intelligence.” *The Telegraph*, August 31, 2015. http://www.telegraph.co.uk/news/uknews/defence/11830594/British-spies-trawl-Ashley-Madison-leak-for-intelligence.html.

Feng, E. “In China, a New Call to Protect Data Privacy.” *NPR*, January 5, 2020. https://www.npr.org/2020/01/05/793014617/in-china-a-new-call-to-protect-data-privacy?t=1600710014451.

Garrie, D., and I. Byhovsky. “Privacy and Data Protection in Russia.” *Journal of Law and Cyber Warfare* 5, no. 2 (2017): 241–242. https://www.jstor.org/stable/26441276.

Gioe, D. V. “Handling HERO: Joint Anglo-American Tradecraft in the Case of Oleg Penkovsky.” In *An International History of the Cuban Missile Crisis*, edited by D. V. Gioe, L. Scott, and C. Andrew, 135–175. 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 R. Dover, H. Dylan, and M. Goodman, 213–228. London: Palgrave Macmillan, 2017.

Gordievsky, O. *Next Stop Execution: The Autobiography of Oleg Gordievsky*. London: Endeavour Media, 2018.

Greenberg, A. “Here’s a Spy Firm’s Price List for Secret Hacker Techniques.” *Wired*, November 18, 2015. https://www.wired.com/2015/11/heres-a-spy-firms-price-list-for-secret-hacker-techniques/.

Greenberg, A. “How the CIA Can Hack Your Phone, PC, and TV (Says WikiLeaks).” *Wired*, March 7, 2017. https://www.wired.com/2017/03/cia-can-hack-phone-pc-tv-says-wikileaks/.

Greenwald, G., and E. MacAskill. “NSA Prism Program Taps in to Use Data of Apple, Google and Others.” *The Guardian*, June 7, 2013. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Grey, S. *The New Spymasters: Inside Espionage from the Cold War to Global Terror*. New York: Viking, 2015.

Heath, J. “Riot Finally Enables Voice Chat for Russian Players in VALORANT.” *Dot Esports*, June 9, 2021. https://dotesports.com/valorant/news/riot-enables-voice-chat-for-russians-players-valorant.

Hoffman, D. E. *The Billion Dollar Spy: A True Story of Cold War Espionage and Betrayal*. London: Icon Books, 2017. Kindle.

Holm, R. *The Craft We Chose: My Life in the CIA*. Oakland: Mountain Lake Press, 2011.

Judah, B. “Putin’s Coup: How the Russian Leader Used the Ukraine Crisis to Consolidate His Dictatorship.” *Politico*, October 19, 2014. https://www.politico.com/magazine/story/2014/10/vladimir-putins-coup-112025_full.html#.WJo84H9yXE9.

Kelion, L. “WhatsApp’s Privacy Protections Questioned After Terror Attack”. *BBC News*, March 17, 2017. https://www.bbc.co.uk/news/technology-39405178.

Kupfer, M., and M. Bodner. “Spy Games: How the Spectre of Surveillance Impacts Moscow’s Foreigners.” *The Moscow Times*, January 19, 2017. https://themoscowtimes.com/articles/spy-games-how-the-spectre-of-surveillance-impacts-the-lives-of-moscows-foreigners-56865.

Lewis, J. “How Spies Used Facebook to Steal NATO Chiefs’ Details.” *The Telegraph*, March 10, 2012. https://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefs-details.html.

Liao, S. “China’s Education Group Releases a Cartoon Encouraging Kids to Embrace Counterespionage.” *The Verge*, November 7, 2017. https://www.theverge.com/2017/11/7/16617494/china-national-security-spying-propaganda-cartoon-education.

Lokhov, P. “How and Why the Russian Military Puts Soldiers in Jail for Using Smartphones and Social Media.” *Meduza*, August 6, 2019, https://meduza.io/en/feature/2019/08/06/how-and-why-the-russian-military-puts-soldiers-in-jail-for-using-smartphones-and-social-media.

Loucaides, D. “The Kremlin Has Entered the Chat.” *Wired*, February 2, 2023. https://www.wired.com/story/the-kremlin-has-entered-the-chat/.

Lowenthal, M. M. *Intelligence: From Secrets to Policy*. 7th ed Kindle. Thousand Oaks: CQ Press, 2017

Lunden, I. “Russia Says ‘Nyet’ Continues LinkedIn Block After It Refuses to Store Data in Russia.” *TechCrunch*, March 7, 2017. https://techcrunch.com/2017/03/07/russia-says-nyet-continues-linkedin-block-after-it-refuses-to-store-data-in-russia/?guccounter=1.

Mackinnon, A. “Hackers Turn the Tables on Russia.” *Foreign Policy*, January 28, 2019. https://foreignpolicy.com/2019/01/28/hackers-turn-the-tables-on-russia-hacking-leaking-cyber-documents-wikileaks/.

Marchetti, V., and J. D. Marks. *The CIA and the Cult of Intelligence*. London: Jonathan Cape, 1974.

Mattis, P. “Virtual Espionage Challenges Chinese Counterintelligence.” *The Jamestown Foundation*, May 7, 2014. https://jamestown.org/program/virtual-espionage-challenges-chinese-counterintelligence/.

Mazetti, M., and J. Elliot. “Spies Infiltrate a Fantasy Realm of Online Games.” *The New York Times*, December 9, 2013. 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.

McLaughlin, J., and Z. Dorfman. “At the CIA, a Fix to Communications Systems That Left Trail of Dead Agents Remains Elusive.” *The Huffington Post*, December 6, 2018. https://www.huffpost.com/entry/at-the-cia-a-fix-to-communications-system-that-left-trail-of-dead-agents-remains-elusive_n_5c094117e4b069028dc7696a.

Meduza. “Russia’s State Duma Just Approved Some of the Most Repressive Laws in Post-Soviet History.” June 24, 2015. https://meduza.io/en/feature/2016/06/24/russia-s-state-duma-just-approvedsome-of-the-most-repressive-laws-in-post-soviet-history.

Mendez, A. J., and M. McConnell. *The Master of Disguise: My Secret Life in the CIA*. New York: Harper Collins, 2007. Kindle.

Mendez, A. J., J. Mendez, and M. Baglio. *The Moscow Rules: The Secret CIA Tactics That Helped America Win the Cold War*

Merzlikin, P. "'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 Sentenced to 13 Years for Treason." *Meduza*, July 31, 2019. https://meduza.io/en/feature/2019/07/31/i-d-be-willing-to-work-against-this-government-with-satan-himself.

Miller, G. "As Russia Reasserts Itself, U.S. Intelligence Agencies Focus Anew on the Kremlin." *The Washington Post*, September 14, 2016. https://www.washingtonpost.com/world/nationalsecurity/as-russia-reasserts-itself-us-intelligence-agencies-focus-anew-on-thekremlin/2016/09/14/cc212c62-78f0-11e6-ac8ecf8e0dd91dc7_story.html?postshare=371473956824384&tid=ss_twbottom&utm_term=.d8941ad4f02e#comments.

Miller, G., E. Nakashima, and A. Entous. "Obama's Secret Struggle to Punish Russia for Putin's Election Assault." *The Washington Post*, June 23, 2017. https://www.washingtonpost.com/graphics/2017/world/nationalsecurity/obama-putin-election-hacking/?utm_term=.73bfdde12b13.

Morgus, R. "The Spread of Russia's Digital Authoritarianism." In *Artificial Intelligence, China, Russia and the Global Order*, edited by N. D. Wright, 89–97. Maxwell: Air University Press, 2019.

National Security Strategy, The White House, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

Newman, L. H. "The CIA Sets Up Shop on Tor, the Anonymous Internet." *Wired*, May 7, 2019. https://www.wired.com/story/cia-sets-up-shop-on-tor/#:~:text=On%20Tuesday%2C%20the%20CIA%20announced,that%20uses%20its%20own%20URLs.

Newton, C. "How China Complicates Apple's Chest-Thumping About Privacy." *The Verge*, October 25, 2018. https://www.theverge.com/2018/10/25/18020508/how-china-complicates-apples-chest-thumping-about-privacy.

Nicas, J., R. Zhong, and D. Wajabayashi. "Censorship, Surveillance and Profits: A Hard Bargain for Apple in China." *The New York Times*, June 17, 2001. https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html.

Nossiter, A., D. E. Sanger, and N. Perlroth. "Hackers Came, but the French Were Prepared." *The New York Times*, May 9, 2017. https://www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html.

NSA. "Exploiting Terrorist Use of Games & Virtual Environments." Published by Cryptome, December 9, 2013. Accessed June 15, 2022. https://cryptome.org/2013/12/nsa-spy-games.pdf.

Office of the Director of National Intelligence. "Know the Risk Raise Your Shield: NSCS Awareness Materials." June 15, 2022. https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield.

Of Justice, D. "United States of America V. Jun Wei Yeo, Also Known as Dickson Yeo." Accessed June 15, 2022. https://www.justice.gov/opa/press-release/file/1297486/download.

Omand, D. "Understanding Digital Intelligence and the Norms That Might Govern It". In *Global Commission on Internet Governance Paper Series: No. 8*¸ 2015. https://www.cigionline.org/sites/default/files/gcig_paper_no8.pdf.

Panel at Third Ethos and Profession of Intelligence Conference held at the George Washington Center for Cyber and Homeland Security. 2016. "CIA-GW Intelligence Conference: Panel on the View from Foreign Intelligence Chiefs." September 20. Youtube video, 57: 48. https://www.youtube.com/watch?v=yefBv7Q3sv0 .

Pepitone, J. "China is 'Leading Suspect' in OPM Hacks, Says Intelligence Chief James Clapper." *NBC News*, June 25, 2015. http://www.nbcnews.com/tech/security/clapper-china-leading-suspect-opm-hack-n381881.

Poitras, V. L., M. Rosenbach, and H. Stark. "GCHQ Monitors Diplomats' Hotel Bookings." *Der Spiegel*, November 17 2013. http://www.spiegel.de/international/europe/gchq-monitors-hotel-reservations-to-trackdiplomats-a-933914.html.

Reuters, "Digitizing the Cia: John Brennan's Attempt to Lead America's Spies into the Age of Cyberwar." November 2, 2016. https://www.reuters.com/investigates/special-report/usa-cia-brennan/.

Reuters, "Putin Tells Russia's Tech Sector: Ditch Foreign Software or Lose Out." September 8, 2017. https://www.reuters.com/article/russia-it-software-idUSL8N1LP4IC.

Russel, R. L. *Sharpening Strategic Intelligence: Why the CIA Gets It Wrong and What Needs to Be Done to Get It Right*. New York: Cambridge University Press, 2007. Kindle.

Samuel, H. "Chinese Spies Fooled 'Hundreds' of Civil Servants and Executives, France Reveals." *The Telegraph*, October 23, 2018. https://www.telegraph.co.uk/news/2018/10/23/chinese-online-spies-fool-hundreds-totally-unprepared-top-french/.

Sanger, D. E. "U.S. Decides to Retaliate Against China's Hacking." *The New York Times*, July 31, 2015. https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html.

Sargsyan, T. "Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security." *International Journal of Communication*, no. 10 (2016): 2225–2229. https://ijoc.org/index.php/ijoc/article/viewFile/3854/1648.

Satter, R. "Chinese Cybersecurity Company Accuses CIA of 11-Year-Long Hacking Campaign." *Reuters*, March 3, 2020. https://www.reuters.com/article/us-china-usa-cia-idUSKBN20Q2SI.

Sheymov, V. *Tower of Secrets: A Real Life Spy Thriller*. New York: Harper, 2012.

SIS. "Sharing Information Securely." March 29, 2023. https://www.sis.gov.uk/share-information-securely.html.

Soldatov, A., and I. Borogan. "In Ex-Soviet States, Russian Spy Tech Still Watches You." *Wired*, December 21, 2012. https://www.wired.com/2012/12/russias-hand/.

Soldatov, A., and I. Borogan. "Russia's Surveillance State." *World Policy Journal* 30, no. 3 (2013): 23–30. doi:10.1177/0740277513506378.

Soldatov, A., and I. Borogan. *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*. New York: Public Affairs, 2015. Kindle.

Stein, J. "The Russian Spy Who Came in Through the Email." *Newsweek*, July 3, 2015. https://www.newsweek.com/russian-spy-through-email-312104.

Sudakov, D. "Russia May Block Whatsapp, Viber, Telegram Even Tomorrow.", *Pravda*, May 2, 2017. http://www.pravdareport.com/business/companies/02-05-2017/137639-messaging_service_russia-0/.

Sukhankin, S. "Russia on the Verge of a 'Cyber Purge?'" *The Jamestown Foundation*, February 9, 2017. https://jamestown.org/program/russia-verge-cyber-purge/.

The Telegraph. "British and US Spies at Risk After Wikileaks Publishes Top-Secret CIA Spyware Document". May 20, 2017. https://www.telegraph.co.uk/news/2017/05/20/british-us-spies-risk-wikileaks-publishes-top-secret-cia-spyware/.

The Telegraph, "CIA Agent 'Detained in Moscow': His 'Letter' in Full." May 14, 2013. http://www.telegraph.co.uk/news/worldnews/europe/russia/10056972/CIA-agent-detained-in-Moscow-his-letter-in-full.html.

Tidy, J. "Security Warning After Sale of Stolen Chinese Data." *BBC News*, July 8 2022. https://www.bbc.co.uk/news/technology-62097594.

Turovsky, D. "Moscow's Cyber-Defense: How the Russian Government Plans to Protect the Country from the Coming Cyberwar." *Meduza*, July 19 2017. https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense.

Van Cleave, M. "Chinese Intelligence Operations and Implications for U.S. National Security." Statement for the Record for *U.S. China Economic and Security Review Commission*, 2019, 1–10. http://www.uscc.gov/sites/default/files/Michelle%20Van%20Cleave_Written%20Testimony060916.pdf.

Wallace, R. "A Time for Counterespionage." In *Vaults, Mirrors, & Masks: Rediscovering U.S. Counterintelligence*, edited by J. E. Sims and B. Gerber, 101–124. Washington: Georgetown University Press, 2008.

Wallace, R., and H. K. Melton. *C.I.A. Manual of Trickery and Deception*. London: Harper Collins, 2009.

Wallace, R., H. K. Melton, and H. R. Schlesinger. *Spycraft: Inside the Cia's Top Secret Spy Lab*. London: Bantam Press, 2008.

Watkins, A. "China Grabbed American as Spy Wars Flare." *Politico*, November 10, 2017. https://www.politico.com/story/2017/10/11/china-spy-games-espionage-243644.

WikiLeaks. "Vault 7: CIA Hacking Tools Revealed". Accessed June 15, 2022. https://wikileaks.org/ciav7p1/index.html.

WikiLeaks. "Vault 7: Projects". Accessed June 15, 2022. https://wikileaks.org/vault7/.

Wikileaks, "Weeping Angel (Extending) Engineering Notes." Accessed January 15, 2023. https://wikileaks.org/ciav7p1/cms/page_12353643.html.

Wilder, U. M. "The Psychology of Espionage." *Studies in Intelligence, CIA* 61, no. 2 (2017): 19–36.

Wong, S. -L., and M. Martina. "China Adopts Cyber Security Law in Face of Overseas Opposition." *Reuters*, November 7, 2016. https://www.reuters.com/article/us-china-parliament-cyber/china-adopts-cyber-security-law-in-face-of-overseas-opposition-idUSKBN132049.

Yahoo! News. "Russia Busts Pair 'Trying to Sell CIA Fake Secrets." September 20, 2016. https://news.yahoo.com/russia-busts-pair-trying-sell-cia-fake-secrets-182012535.html.

Yang, S. "China to Ban Online Gaming, Chatting with Foreigners Outside Great Firewall: Report." *Taiwan News*, April 15, 2020. https://www.taiwannews.com.tw/en/news/3916690.

Yang, Y. "China's Cyber Security Law Rattles Multinationals." *Financial Times*, May 30, 2017. https://www.ft.com/content/b302269c-44ff-11e7-8519-9f94ee97d996.

Zakharov, A. "Russian Data Theft: Shady World Where All is for Sale." *BBC News*, May 27, 2019. https://www.bbc.co.uk/news/world-europe-48348307.

Zetter, K. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers, 2014.

Zhou, Z. "China's Comprehensive Counter-Terrorism Law." *The Diplomat*, January 23, 2016. https://thediplomat.com/2016/01/chinas-comprehensive-counter-terrorism-law/