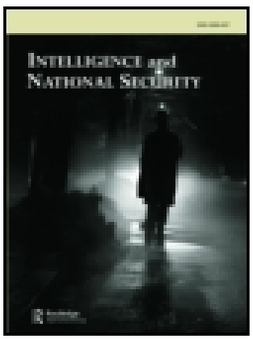
Hard target espionage in the information era : new challenges for the second oldest profession

Cunliffe, KS

http://dx.doi.org/10.1080/02684527.2021.1947555



Intelligence and National Security

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

Hard target espionage in the information era: new challenges for the second oldest profession

Kyle S. Cunliffe

To cite this article: Kyle S. Cunliffe (2021): Hard target espionage in the information era: new challenges for the second oldest profession, Intelligence and National Security, DOI: 10.1080/02684527.2021.1947555

To link to this article: https://doi.org/10.1080/02684527.2021.1947555

Published online: 07 Jul 2021.

INTELLIGENCE AND NATIONAL SECURITY
https://doi.org/10.1080/02684527.2021.1947555

Routledge
Taylor & Francis Group

ARTICLE

OPEN ACCESS Check for updates

Hard target espionage in the information era: new challenges for the second oldest profession

Kyle S. Cunliffe

ABSTRACT

Reliable and well positioned human sources are essential for the US and its allies in an era of declining relations and rising tensions with China and Russia. The recruitment and handling of spies is essential if the US and its allies are to cool relations carefully, enact sound policy and curb the relentless intelligence operations of their adversaries. However, despite the superficially more open borders of China and Russia, technological advances have made the threat of street surveillance to the recruitment and handling of agents today as acute as it was in Cold War "denied area" states. This paper assesses the degree of street surveillance in contemporary Russia and China – including the impact of biometrics and online data history on the defensibility of cover and the severity of advanced CCTV networks – and the solutions intelligence agencies might adopt to address these problems. Despite the possibilities cyberspace offers espionage – for instance, by reducing the need for face to face meetings between intelligence officers and agents – the paper establishes the limitations of technological answers and argues that Western intelligence officers are entering a new era of Moscow and Beijing Rules in which they are more essential than ever and yet need to operate with absolute caution.

Introduction

In 2018, the Trump administration declared Russia and China to be the main security concerns of the United States, not terrorism.[1] This move was hardly unanticipated. As former Defence Secretary James Mattis claimed, declining relations and rising tensions with these 'revisionist powers' have increasingly challenged US hegemony.[2] But as military and intelligence resources are steered accordingly towards Beijing and Moscow, Humint, meaning in this case espionage – the recruitment and handling of spies – must play a primary role. The most important secrets, including the aims and intentions of President Xi and President Putin, are likely contained either in the minds of a select few or in heavily guarded vaults.[3] Simply put, if the US and its allies are going to cool relations, enact sound policy, and curb the relentless intelligence operations of their adversaries, they are going to need reliable and well positioned human sources.

Yet in order to recruit and handle these human sources (better known as agents or spies), today's intelligence officers must compete with the rising threat of street surveillance, a threat that has parallels with the Cold War. Street surveillance, meaning the physical observation of intelligence officers, is the Achilles Heel of espionage, allowing contacts, movements, and tradecraft to be mapped out.[4] To avoid their watchers, intelligence officers run countersurveillance techniques, which in turn pushes up the amount of resources that counterintelligence must invest to keep a single person under observation.[5] Rampant street surveillance was a hallmark of the Cold War's 'denied area' states: restricted borders limited the intake of potentially suspicious foreigners into the

CONTACT Kyle S. Cunliffe Kscunliffe99@outlook.com

Soviet Union, while massive KGB resources put the few who arrived under intensive observation.[6] Everyone from students to tourists were watched to some degree, and those most likely to be intelligence officers – especially diplomats – were barely able to escape the KGB's pervasive glare. Surveillance was so endemic, that the West developed a series of guidelines, known as Moscow Rules, to help intelligence officers navigate Soviet turf – most notably rule 1 'Murphy is right', which might have been better expressed as *assume nothing but the worst*.[7] But at their heart, Moscow Rules reflect a period of intense struggle, where every agent was hard won.

The laxing of Russian and Chinese borders in the post-Cold War world brought about greater opportunities for Western intelligence officers. Tourists and businessmen could travel to their major cities with relative ease, with a larger footprint of international travellers putting new strains on surveillance while offering more wiggle room for foreign operatives. However, today the advantages offered by these more open societies must be weighed against emerging technological threats. In recent years, technological developments have created new challenges to intelligence officers' cover (the fake identities they use to enter and socialise in foreign environments), potentially allowing surveillance to function with unprecedented speed and efficiency. As argued by the former head of SIS, Alex Younger, today's intelligence officers face an 'existential threat' brought about by the information age.[8] These technological challenges have already been documented to some extent by scholars and former practitioners, including former CIA case officer David Gioe and former deputy head of SIS, Nigel Inkster, but have not received sustained examination in the context of specific hard targets.[9] This paper thus attempts to examine the state of street surveillance in contemporary Russia and China, alongside the solutions that intelligence agencies might adopt to address the problems it presents. It aims to show that the West faces a new and fraught era of Moscow/Beijing Rules with no easy resolution and dire implications for the value of espionage.

Russia and the FSB

The Russian government's willingness to invest vast resources in surveillance is 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.[10] The collapse of the Soviet Union brought new problems for Russian counterintelligence, as internal chaos, burgeoning organized crime, growing numbers of foreign intelligence officers, war in Chechnya, and low wages, stretched its new domestic security agency, the FSB, to the utmost.[11] 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.[12] And whereas the worst impulses of the KGB were reined in by party control, its successor is a far more autonomous beast, more loyal to Putin than to the state.[13]

Since his tenure in the late 1990s as director of the FSB, Putin has increasingly called for greater effort in tackling foreign espionage.[14] Declining relations with the West have seen these fears escalate, with foreign spying rising to the state's top security priority.[15] 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.[16] 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'.[17] But regardless of whether the Kremlin truly perceives foreign intelligence as underpinning domestic opposition, the threat of foreign espionage and the surveillance of foreign operatives is central to Russian security. This is underscored by the sheer size of the FSB, which in 2013 boasted of manpower between 200,000 and 300,000 strong, a number which has since risen to almost 400,000 – a stark contrast to the meagre 13,000 in Russia's foreign intelligence service (SVR).[18]

Given these numbers, anyone suspected of being an intelligence officer in Russia must expect unrelenting scrutiny. According to 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 media reports, 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] Such unpleasant incidents only worsened in the aftermath of Russia's incursions into the Ukraine and Crimea. As detailed in a report by Estonia's Teabeamet intelligence agency, the tactics used by Russian security services against foreign officials have escalated in danger, recklessness and audaciousness, including burglaries, intimidation, harassment, defamation, physical assault, and even drink spiking.[22]

In some cases, this behaviour 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. The attack was allegedly provoked when the CIA officer successfully lost his tail, infuriating the FSB who responded by inflicting injuries severe enough to merit an immediate medical flight out of Moscow.[23] Previously, aggressive harassment of this nature was mostly reserved for intelligence officers who contentiously provoked their watchers, but evidently this unwritten rule of espionage is being ignored.[24] 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 of U.S. diplomats in Moscow was irresponsible, reckless, intolerable and needed to stop'.[25] Despite this effort, within a year US diplomats and their families were reporting further acts of intimidation and harassment by Russian security services throughout Moscow and Europe.[26]

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 the 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'.[27] 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. However, 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'.[28] Simply put, if intelligence offers are to meet sources with credible access to classified information, they will likely have to do so in Moscow, against the full force of Russian counterintelligence.

China and the Ministry of State Security

The state of affairs in China has drawn considerably less media attention, but it is clear that Beijing also 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.[29] With the separation, MSS not only took the lead on foreign intelligence gathering (which it also absorbed from the Investigation Department), it also took the helm of counterintelligence missions including street surveillance and technical eavesdropping.[30] The MPS is still responsible for policing

and public order, but the MSS absorbed all offensive and defensive aspects of intelligence under one roof. In recent years, owing in part to China's large and growing international community, the budgets of MPS and MSS have grown considerably.[31] By 2010, China's internal security budget already outstripped its immense military modernization budget by several billion, rising to 111 USD billion in 2012.[32] While the portion of that funding spent on counterintelligence is unclear, it emphasizes China's voracious appetite for security.

Even by the end of the Cold War, concerns about 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 international journalists and business travellers under surveillance.[33] By the 1990s, Chinese policymakers exhibited 'what might be described in Western terms as a paranoiac fear of foreign influence', and that fear has not abated amongst Chinese policymakers.[34] 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. 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, 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'.[35]

As analyst Scot Tanner told *The New York Times*, the law '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'.[36] Since 2014, street surveillance against intelligence officers and diplomats in Beijing has grown in intensity and aggression. 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'.[37] Although the official described Chinese surveillance as more 'subtle' than their Russian counterparts, some incidents show a more dangerous trend. 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'.[38] 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). In 2016, an official from the US consulate in Chengdu was kidnapped, interrogated, and forced to confess to acts of treachery by plain-clothes 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.

Moreover, akin to Russia, travel restrictions ensure that if intelligence officers want to meet highly valued Chinese sources they will probably have to do so in hostile conditions. Currently, both serving and ex-Politburo members are not allowed to travel abroad without permission, including China's former presidents. As 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'.[39] Consequently, like their colleagues in Moscow Station, foreign intelligence officers in China 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.

Biometric checkpoints & secondary screening

The street surveillance threats developing in Russia and China are only becoming more acute as a result of rapid advances in technology. Traditionally, street surveillance has been hampered by the

manpower required to keep just one person under observation. Even narrowing down the list of potential suspects was a difficult process. It was usually easier in the case of diplomatic travellers but harder for those under nonofficial cover (such as businessmen who were not contained inside a single embassy). But emerging and proliferating technologies, most notably biometrics, are streamlining the entire surveillance process.

From the moment an undercover traveller arrives in a Moscow or Beijing airport, they face biometric checkpoints. Fingerprint, iris, and facial scanners inside airports essentially tie a person's biological attributes to a specific identity, which is naturally problematic for intelligence officers under cover profiles.[40] As one US intelligence officer notes 'it's a one-time thing – one and done. 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.'[41] Although practitioners have warned for some time about the risks of biometrics, in many cases these threats are overblown. Leaked documents by the CIA, for example, pertaining to the EU's Schengen area, note that European countries use biometrics primarily for immigration and law enforcement purposes, not counterintelligence, and that CIA officers rarely fit the targeted profile – in other words, the EU's systems pose 'minimal identity threat' to its operatives.[42] However, hard targets who prioritize counterintelligence are likely to use biometric systems to their advantage and it is perhaps unsurprising that Russia and China are voracious adopters. In 2017, China began a nationwide programme to fingerprint all foreign travellers entering the country.[43] While, in 2014 Russia adopted Executive Order 735, requiring collection of biometric data (fingerprints) of 'all foreign nationals and stateless persons for each of their applications for Russian visa', although the Ministry of Foreign Affairs was sure to insist that its actions followed global norms.[44]

This is true to an extent. In keeping with international norms, Russia and China do not collect biometrics when issuing diplomatic visas.[45] However, any diplomat pulled aside for airport 'secondary screening' – a process of additional scrutiny by security officers for select travellers – may have their biometrics tested. As described by leaked CIA documents released by Wikileaks, 'the 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'.[46] 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 as an excuse for airport officials to elicit bribes.[47] In short, there are multiple reasons why operatives might be led to secondary screening. Indeed, one CIA officer was even screened, they suspect, for wearing 'overly casual dress inconsistent with being a diplomatic-passport holder'.[48]

If pulled into secondary screening, the undercover traveller then faces the problem of life history data. Simply put, today's business or diplomatic professionals are expected to exist in cyberspace, and security officers armed with laptops can check social and professional networks for these online trappings. If this information is missing, or so limited as to appear manufactured, then the intelligence officer will likely fall under immediate suspicion.[49] Although security officers can only examine this data *if* they have access to it, some countries get round this problem, including the US and Russia, by requiring certain visa travellers to surrender social media history in advance – five years' worth in the US case.[50] Security officials may also force visitors to reveal their accounts on the spot, or even tamper with phones and laptops to access personal data. China, as a case in point, has an established reputation for tampering with visitors' devices at the border – even planting malware on specific machines to monitor them afterwards.[51]

Social media also presents a problem through rapid advances in facial recognition. 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 friends and family, drawing a link between his fabricated and real identities.[52] What's more, as artificial intelligence and machine learning evolve, so too do the risks. A long-forgotten graduation photograph posted on

a classmate's blog, could be enough to unravel the deepest of cover – and all the CI officer needs to do is upload a photograph to an app. One such facial recognition tool is Russia's *FindFace*, which matches social media photos with around seventy percent reliability.[53] The tool's developers tellingly stated that 'if the FSB were to get in touch, of course we'd listen to any offers they had'.[54]

Further scrutiny through stolen data

Some data, however, is stored in databases held by commercial and government organisations, rather than on personal devices. This information is harder to access, but is not beyond the capabilities of Russian and Chinese counterintelligence. This was made clearly apparent through China's 2016 hack of the Office of Personnel Management, which included, among sensitive vetting forms, approximately 1.1 million US federal employees fingerprints.[55] 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 fix in the world of intelligence.'[56] 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. Fortunately, CIA officers were not included in the breach as Langley holds its own records, but 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 still 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'.[57]

Yet the OPM hack underscores a larger threat, with US experts concerned that Chinese security services are building a vast database of Americans, using information stolen through hacking.[58] These suspicions have been fed by anonymous CCP sources of the *Epoch Times*, which claimed that Chinese security services and technology companies are collating an enormous database of foreigners using data collected from covert activities.[59] Similar sentiments were expressed by US counterintelligence officials interviewed by the *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 applications, airline records and medical insurance forms'.[60] The article, supplemented by extensive interviews, asserted that vast amounts of stolen and legally acquired information, including travel records, financial details, medical history, social media accounts, and other forms of personal data, were being converted into actionable counterintelligence datasets for identifying undercover travellers. For example, former NSA officer David Aitel told *Business Insider* how the flight patterns stolen in the United Airlines hack could be compared against other stolen databases, including OPM, to identify operatives who travelled to and from CIA headquarters in Langley.[61] Thus, even if the undercover traveller carries a convincing biometric and cyber profile, their cover can still be unravelled in secondary screening by data that is far beyond their own control.

Escaping the streets and CCTV

Of course suspicious biometric and data history does not immediately infer guilt. Biometric systems, as a case in point, have a small chance of false positives and false negatives, while it is hard to justify cancelling a person's visa on the grounds that they only have a six month old LinkedIn account.[62] Instead, it is far more likely that an undercover traveller will be allowed to pass through an airport, but marked as a person-of-interest and a target for further surveillance.. Once in the operational theatre, today's operatives need to compete with more than just their physical tails – they will also need to compete with blanket CCTV coverage. Even basic CCTV has caused severe problems for undercover travellers, as epitomized by the Israeli assassination team responsible for the death of

Mahmoud Al-Mabhouh, a team whose movements and elaborate disguises were rapidly unravelled by CCTV cameras spread throughout Dubai's luxury hotels.[63] Perhaps unsurprisingly, China, with its vast populace, has a voracious appetite for CCTV, operating around 170 million cameras in 2017 alone, a figure that was set to have risen to 400 million by 2020.[64] It also claims to have achieved one-hundred prevent coverage of Beijing, while some regions use networks of cameras dissected into interconnected grids.[65] 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.[66]

China is also rolling out a more advanced network of CCTV combined with facial recognition software to identify targets automatically. As disclosed in a *BBC News* report on 10 December 2017, the system was first 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.[67] This complex system includes the prolific application of cameras equipped with artificial intelligence software, which is able to match individual faces in a crowd, as well as 'estimate age, ethnicity and gender'. As one of the technology's architects explained: '[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.' 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 USD billion in similar technologies on a national level.[68]

Similarly, by 2017 Moscow already boasted around 146 thousand surveillance cameras.[69] And according to investigative researchers, Soldatov and Borogan, the Russian authorities are trialling an advanced CCTV network of their own, using 'multibiometric systems for identifying individuals in real time'.[70] This technology means the camera 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'.[71] One trial in Moscow's metro stations, being carried out under the auspices of the FSB, compares captured photographs against Interior Ministry databases, allegedly scanning 10 million images in seven seconds, and, according to its founder, can 'pinpoint a person's whereabouts at a given moment with an accuracy of up to 96%'.[72] Variations of this system are 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 double check their images for an exact match.[73] As of 2020, this approach seems to have been embraced, with the authorities planning to expand cameras throughout trams, underground railways, and outside apartment buildings and public spaces in various cities, including in the capital.[74]

Coming to terms with the new reality

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 option, for example, is that operatives could circumvent biometric checkpoints and secondary screening by avoiding major airports. However, if an intelligence officer is to maintain their cover profile, they will probably have to reside in upscale hotels, in keeping with the standards of diplomatic and business travellers – yet those hotels are likely to check customer passports against immigration databases, meaning inconsistencies can still be flagged.[75] Another possibility, as Stein argues, is to manipulate foreign databases with human agents or hacking, to 'change data on demand'.[76] According to *Bellingcat*, Russia's FSB pursued a similar strategy in 2015, pressuring a source dubbed 'Vadim' to manipulate UK visa systems.[77] 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.[78] 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 Russian interest in manipulating the immigration process. This kind of manipulation is of just as much interest to Western intelligence officers, 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.[79]

As an alternative to hacking databases, 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'.[80] But even assuming these highly protected systems could be breached, there may be no way to know whether the event succeeded, posing serious risks, since if the operation failed the consequences could be disastrous.[81] 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 one 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'.[82] Former Mossad operative Michael 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 interim solution.'[83] This approach is problematic, because the sharing of biometric information means that intelligence officers may need to use a single identity in a 'group of countries' – a group that only expands as more countries share biometric data.[84] 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'.[85] 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 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'.[86] In other words, there is no single solution. 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 as a 'golden opportunity'?

It bears emphasising that 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 technical assistance in the field (and also rely on cover) might be identified and blackmailed.[87] But the clearest threat of all is that counterintelligence can identify undercover operatives with speed and precision, and tail them until they meet their sources and agents. Intelligence officers must thus operate under the assumption that they are being watched, turning to alternative tradecraft to reduce their dependency on increasingly dangerous personal meetings. Herein, cyberspace is increasingly heralded as a convenient solution to intelligence officers' woes, by opening new, potentially safer, ways to recruit and handle spies. 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).[88]

The DDI holds a broad range of missions, including developing cutting edge analytical software for making sense of vast OSINT datasets and improving Langley's outdated legacy systems.[89] But despite these supporting functions, the DDI's focus is very much centred on counterbalancing the challenges to intelligence officers' cover, by understanding the threats and opportunities that technology brings. As Brennan explained in a 2016 interview with the Aspens Institute, 'for too long the intelligence community was pushing off technology and saying no, we need to stay clear of it', and as such, the DDI will now consider more carefully 'what are the risks, what are the threats, what are the challenges, but also what are the opportunities?'.[90] That same year, British media reported that SIS was to receive a substantial budget increase, upping its personnel by approximately forty percent, in a move aimed at improving the agency's technological aptitude.[91] As explained by the *Financial Times*, UK intelligence officials believe that technological threats demand 'more fulsome changes to the very nature of spycraft itself'.[92] In a joint 2018 interview with his US and Australian counterparts, the then serving 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.'[93] 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.[94]

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'.[95] But while serving intelligence officers avoid specifying what these changes might look like, former practitioners envisage game changing benefits, potentially allowing spies to be recruited and handled with extraordinary speed and efficiency. They could, for instance, be spotted online with a cursory search of social media, assessed with information gathered through hacking, and handled through encrypted communication platforms.[96]

The limits of cyberspace

Pinning the future of espionage on technology is cause for concern. The simple fact of the matter is that counterintelligence is adaptive, and historical precedent does not lean in espionage's favour. In the Cold War, the CIA tried to best the KGB's Moscow panopticon by investing millions of dollars in cutting-edge tradecraft, not dissimilar to the investment in cyberspace today. But while this led to some game-changing innovations, ultimately the KGB always maintained the upper hand – the CIA did not penetrate the upper echelons of the Kremlin, and as far as the literature indicates, it only managed to recruit and handle one noteworthy agent, named Adolf Tolkachev, *entirely* within the confines of Moscow.[97] SIS fared little better. Although they handled their prized agent, Oleg Gordievsky, safely in Copenhagen, when he returned to Moscow they placed him 'on ice', avoiding unnecessary risks by avoiding communicating with him either interpersonally or impersonally.[98] Consequently, despite innovation, these premier espionage agencies never substantially reduced their dependency on the handful of Soviets who travelled abroad or on those who volunteered their own services.[99]

Some might argue that cyberspace is different – that this time counterintelligence is outmatched by the benefits of technology, but the evidence does not seem to support this proposition. At a minimum, there's the problem of the human dimension since espionage thrives and depends on human bonds. The former chief of the CIA's gadget laboratory, Robert Wallace, writes that today's intelligence officers may run virtual personal meetings with their agents through video-link communications.[100] If secure, that would be an enormous advantage, reducing the need for high-risk meetings in Moscow or Beijing's surveilled streets. Gioe, however, who has case officer

experience, argues that those important bonds cannot be easily replicated through virtual means, since even video communications limit non-verbal cues and lead to an experience that is altogether less rewarding, and generates less trust, than a personal meeting.[101] It is worth noting that both Wallace and Gioe cite the case of Robert Hanssen, who never met his Russian handlers face-to-face. Wallace sees Hanssen's faceless tradecraft as something of a benchmark for modern espionage, but Gioe notes that Hanssen was a professional intelligence officer who 'could dictate the terms and his information was beyond reproach'.[102] In other words, Hanssen was an exception, and most agents are still going to need to meet from time to time. And in the current climate, where the FSB seems more than willing to take extreme measures against perceived traitors – such as the attempted poisoning of Sergei Skripal – this need for interpersonal trust is all the more important.

While personal meetings will be necessary in most cases, dependency on face-to-face contact can still be reduced by sound tradecraft. For instance, rather than identifying targets through lengthy face-to-face rapport building, instead they might be spotted and assessed through information gathered on social networks like Facebook, or by hacking personal devices or larger databases.[103] With enough data, advances in machine learning might automatically filter out the best candidates, rapidly speeding up the spotting and assessment process.[104] But even more surgical approaches, aimed at specific targets, can be invaluable to recruitment. In a body of documents dubbed Vault 7, Wikileaks disclosed a whole suite of CIA hacking toolkits focused on hacking targets' personal devices, including phones, laptops, and even smart televisions.[105] And once a target is found, online communications could be used to lay the groundwork of a relationship. Edward Lucas makes the case that even online video games could be used to cultivate sources before an operative delivers a face-to-face pitch (e.g., 'would you like to work for the CIA?').[106] In theory, these capabilities are a huge boon for recruiting agents, and resolve a lot of the intelligence community's problems, but it stands to reason that hard target states, who prioritize security, will not allow such an obvious hole in their defences to exist with impunity.

Scholars need only look to draconian data laws being implemented in Russia and China to see a clamp down on the freedoms that cyberspace supposedly affords. These laws essentially force mainstream internet companies into a dilemma – either relocate their servers within Russian and Chinese borders, where their information can be accessed and regulated by state security services, or face nationwide blocking.[107] Foreign intelligence officers operating in cyberspace are high on the security agenda – China has implemented a national propaganda campaign, including anti-spy cartoons tailored towards young audiences, which forewarn of the dangers of foreigner operatives recruiting Chinese nationals.[108] In addition, both states, who are concerned about rampant data leakage and foreign hacking, are taking measures to improve their cyber defences and better protect personal data.[109] In practice, this means that recruiting and learning about spies online may be harder, or less secure, than is often supposed. In the Soviet Union, the expression 'this is not a telephone call' was well known, and expressed a universal fear that the state security services may be listening, but in this growing climate of cyber-surveillance those fears are just as entrenched today.[110] Thus, those with access to classified information are likely to be less inclined to say or share anything sensitive by insecure means.

Cyberspace may be of greater aid to handling than to recruitment. For instance, advances in encryption, including anonymising tools such as The Onion Router (Tor) which grants access to the dark web, have been described as 'nothing short of a tradecraft revolution'.[111] Other practitioners have noted that the shift from paper-based to digital documents means that a single spy may be able to collect more secrets than ever before. They cite the case of Edward Snowden, who illegally copied thousands of classified documents from NSA systems in Hawaii, smuggling them out with a USB thumb drive.[112] If handling were largely relegated to online means, and if agents could cement their trustworthiness by supplying thousands of digital secrets, reliance on face-to-face contact would arguably plummet – perhaps being reserved for giving agents a much needed boost of morale.

But again, there's enormous room for doubt. Headlines from 2018 claim swathes of agents in China and Iran (and potentially Russia) were arrested and executed because of technical flaws in the CIA's bespoke online covert communication system.[113] The system, which allowed intelligence

officers to communicate with agents anywhere in the world, was allegedly foiled at the behest of an Iranian double agent and by simple Google key-word searches.[114] And yet the fact that the system existed implies that commercial solutions were not deemed particularly secure, and even now a fix – which apparently has not been found – is expected to cost billions of dollars.[115] Moreover, while Snowden did indeed cause enormous damage with his unchecked access to classified systems, his case may be better seen as an exception, not a rule. Snowden operated from a Hawaiian branch that was still in the process of updating its security measures, and NSA personnel insist that if he had worked in NSA headquarters at Fort Meade, he would have been caught before ever getting his data out of the building.[116] In a paranoid hard-target state, it would be a mistake to assume that government workers have unchecked access to vast amounts of classified data. Indeed, Russia allegedly keeps some of its most important secrets on paper to curb any Snowdens of its own.[117]

These factors, and more, bring into question whether cyberspace really is the 'golden opportunity' that espionage agencies require. But if intelligence agencies cannot resolve the street-surveillance problem with innovation, then their options are limited. They could return to traditional practices, which were generally painstakingly difficult to pull off securely, and required a great deal of planning and patience.[118] It is perhaps indicative that due to the failings of CIA's covert communication system mentioned above, operatives are reportedly returning to old-fashioned techniques, including burst radio communications and personal meetings. This, in spite of the fact that advocates of these antiquated techniques were, until recently, considered to be 'troglodytes' by their peers.[119] The alternative is for intelligence agencies to pursue their targets on safer soil, limiting the number of agents they can potentially recruit or handle. And, in the absence of perfect solutions, it might otherwise be simpler to adopt SIS's approach with Gordievsky, keeping agents on 'on ice' whenever they are recalled home to Moscow or Beijing – a major problem if agents are recalled indefinitely.

Ultimately, espionage *is* changing, meaning operatives are going to have to adapt to this new reality. They must accept that the defensibility of cover is increasingly waning and that personal meetings in hard target states are unlikely to go unnoticed. And yet policymakers must understand that investment in technology cannot necessarily shift the favour towards their own intelligence agencies. Too much emphasis on the value of cyberspace can lead to unrealistic expectations and, as it stands, cyberspace brings more problems to the table than it seems to resolve. That said, it may be better to spend a great deal of money to secure a handful of opportunities, than to walk into an increasingly dangerous security climate without a fully supported espionage capability. If cyber-enabled tradecraft can provide a single opportunity to recruit a high valued agent – for example, by allowing operatives to notice when a particular Kremlin official is taking a vacation to a country where they may be safely met – then its value pays off. A single agent within the inner circle of President Putin or President Xi may be enough to justify the billions of dollars that Langley is presently spending to resolve its operational woes. Nonetheless, with no easy solutions in sight, intelligence officers are entering a new era of Moscow and Beijing Rules, and will need to operate with absolute caution in these major cities.

Notes

1. *BBC News*, "Mattis: US National Security Focus no Longer Terrorism"
2. *National Security Strategy*.
3. Grey, *The New Spymasters*, 286.
4. Olson, "A Never-Ending Necessity," 81–7.
5. Shulsky and Schmitt, *Silent Warfare*, 109.
6. Mendez and McConnell, *The Master of Disguise*, 221–25.
7. Mendez et al. *The Moscow Rules*, xi.
8. "CIA-GW Intelligence Conference."
9. Regarding technological challenges in hard-target, Edward Lucas has undertaken a preliminary exploration of this area in *Spycraft Rebooted*. For other initial engagements see: Gioe, "The More Things Change,"; Inkster,

"Intelligence Agencies," 45–6; Clark, *Intelligence Collection*; Streeter, "Biometrics and Intelligence Asset Protection".
10. Mendez and McConnell, *The Master of Disguise*, 221–26.
11. Brope, "Russia," 231–34.
12. Galeotti, "Russian Intelligence."
13. Soldatov and Borogan, *The New Nobility*, 4.
14. Ibid., 35–6.
15. "Russia: Implication for UK Defence".
16. "Meeting of Federal Security Service Board."
17. Bateman, "The Political Influence," 400.
18. "Supplementary Written Evidence," 1–3; Lucas, *Deception*, 68.
19. Miller, "As Russia Reasserts Itself".
20. Miller, "Moscow Rules of Espionage Go Global".
21. Rogin, "Russia Is Harassing U.S. Diplomats all over Europe".
22. Teabeamet, "International Security and Estonia," 26.
23. Watkins, "Russia Escalates Spy Games Go Global".
24. Miller, "Moscow Rules of Espionage".
25. *CNN*, "Intel Chief Testifies Amid New Russia Revelations".
26. See note 19 above.
27. Ryzhkov, "Controlling Russians". All further facts and quotations in this paragraph relating to travel bans are drawn from this source.
28. Ryzhkov, "Controlling Russians through Travel Bans".
29. Guo, *China's Security State*, 437.
30. Inkster, "Chinese Intelligence," 48.
31. Mattis, "Beyond Spy vs. Spy," 50.
32. Ibid.
33. Stratfor Global Intelligence, "Intelligence services," 4–9.
34. Eftimiades, *Chinese Intelligence Operations*, Ch. 6, penultimate paragraph.
35. Brookes, "Is China Swarming with Foreign Spies?".
36. Tatlow, "China Approves Security Law".
37. Watkins, "China Grabbed American".
38. Stein, "Chinese Counterspies".
39. Stone Fish. "Why Can't Ex-Chinese Leaders Travel Abroad".
40. Gioe, "The More Things Change," 216–217.
41. Stein, "CIA's Secret Fear".
42. "CIA Advice for US Government Operatives," i.
43. Bright, "China to Start Scanning Foreign Travellers' Fingerprints".
44. The Embassy of the Russian Federation, "About the New Requirement for Foreign Nationals".
45. Mo, "Fingerprinting of Foreign Visitors".
46. CIA, "CIA Assessment on Surviving Secondary Screening," 3.
47. Ibid., 6–11.
48. Ibid., 14.
49. Gioe, "The More Things Change," 218.
50. Mosbergen, "Nearly All U.S. Visa Applicants Now Required to Submit 5-Year Social Media History".
51. Osborne and Cutler, "Chinese Border Guards Put Secret Surveillance App on Tourists' Phones".
52. Mahmood, "Online Social Networks and Terrorism," 85.
53. Walker, "Face Recognition App Taking Russia by Storm May Bring End to Public Anonymity."
54. Ibid.
55. Institute for Critical Infrastructure, "Preparing the Battlefield," 16–17.
56. Ibid.
57. Corera, "The Spies of Tomorrow".
58. Nakashima, "With a Series of Major Hacks".
59. Philipp, "You're on File".
60. Bennett and Hennigan, "China and Russia Are Using Hacked Data".
61. Bertrand, "Russia and China Could Be 'Making It Impossible For The US To Hide'".
62. Streeter, "Biometrics," 11.
63. Inkster, "Intelligence Agencies," 46.
64. *BBC News*, "In Your Face".
65. Yin, "More 'Eyes' Fight Crime in Crowds"; and Callick, "China's All-Seeing Spy Grid."
66. Callick, "China's All-Seeing Spy Grid."
67. "In Your Face: China's All-Seeing State," *BBC News*.

68. Mozur, "Inside China's Dystopian Dreams".
69. McFarland, "146,000 Cameras Monitor Moscow Streets".
70. Soldatov and Borogan, "A Face in the Crowd."
71. Ibid.
72. Ibid.
73. Ibid.
74. Zhumatov, "Russia Expands Facial Recognition."
75. Stein, "CIA's Secret Fear".
76. Stein, "CIA's Secret Fear".
77. *Bellingcat*, "Spies Without Borders".
78. Corera, "Russia "Sought Access to UK Visa Issuing System"".
79. Stein, "CIA's Secret Fear". See also Tucker, *The End of Intelligence*, 83–84; and Lucas, *Spycraft Rebooted*, ch. 6.
80. Streeter, "Biometrics," 16–17.
81. Lucas, *Spycraft Rebooted*, ch. 6.
82. Lord, "Undercover under Threat," 686.
83. Murphy, "How Technology is Changing the Future of Espionage."
84. Gioe, "The More Things Change," 216.
85. Tucker, *The End of Intelligence*, 83; and Jones, "The Spy who Liked Me."
86. Syeed, "CIA Cyber Official Sees Data Flood".
87. Bennett and Hennigan, "China and Russia are Using Hacked Data".
88. Rohde, "Special Report"; Tucker, "CIA Restructuring"; Slick, "Measuring Change at the CIA"; and Lyngaas, "Inside the CIA's New Digital Directorate."
89. "Deputy Director Cohen Delivers Remarks on CIA of the Future at Cornell University."
90. "A Candid Conversation with the Director of the Central Intelligence Agency."
91. Urban, "MI6 Set to Recruit 1,000 Extra Staff".
92. Jones, "The Spy Who Liked Me".
93. "CIA-GW intelligence conference".
94. Ibid.
95. Ibid.
96. Gioe, "The More Things Change," 218–220.
97. Russell, *Sharpening Strategic Intelligence*, 51–52; and Royden, "Tolkachev, a Worthy Successor to Penkovsky".
98. Gioe, "Handling HERO," 169.
99. Garthoff, *A Journey through the Cold War*, 104.
100. Wallace, "A Time for Counterespionage," 114.
101. Gioe, "The More Things Change," 221–222.
102. Wallace, "A Time for Counterespionage," 117; and Gioe, "The More Things Change," 225.
103. Gioe, "The More Things Change," 218.
104. Jensen et al, "Algorithms at War," 532.
105. Shane et al, "Wikileaks Releases Trove of Alleged C.I.A. Hacking Documents."
106. Lucas, *Spycraft Rebooted*, ch. 6.
107. Bauer et al, "Data Localisation in Russia," 2; and Zhou, "China's Comprehensive Counter-Terrorism Law".
108. Liao, "China's Education Group".
109. "China Cracking Down on Data Theft"; Zakharov, "Russian Data Theft"; and Kolomychenko, "Russia, Stung by Intelligence Leaks".
110. Soldatov and Borogan, *The Red Web*, ch. 1.
111. Gioe, "The More Things Change," 220.
112. See note 92 above.
113. Dorfman, "Botched CIA Communications System."
114. Dorfman and McLaughlin, "The CIA's Communications Suffered a Catastrophic Compromise."
115. McLaughlin and Dorfman, "At the CIA."
116. Sanger and Schmitt, "Snowdon Used Low-Cost Tool".
117. Elder, "Russian Guard Service Reverts to Typerwriters".
118. Sano, "The Changing Shape of HUMINT," 79.
119. See note 114 above.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Kyle Cunliffe is a fixed-term lecturer 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.

Bibliography

The Aspen Institute. 2016. "A Candid Conversation with the Director of the Central Intelligence Agency." Streamed live on 30 July 2016. Youtube video, 1:02:12. https://www.youtube.com/watch?v=TRCUO7-IbUE .

Bateman, A. "The Political Influence of the Russian Security Services." *The Journal of Slavic Military Studies* 27, no. 3 (2014): 380–403. doi:10.1080/13518046.2014.932626.

Bauer, M., H. Lee-Makiyama, and V. D. M. Erik. "Data Localisation in Russia: A Self-imposed Sanction." *European Centre for International Political Economy* 6, no. 1–7 (2015). https://ecipe.org/wp-content/uploads/2015/06/Policy-Brief-062015_Fixed.pdf .

BBC News. 2017. "In Your Face: China's All-seeing State." December 10. http://www.bbc.co.uk/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state

BBC News. 2018. "Mattis: US National Security Focus No Longer Terrorism." January. 19. https://www.bbc.co.uk/news/world-us-canada-42752298 .

Bellingcat. 2018. "Spies Without Borders – How The FSB Infiltrated The International Visa System". November 16. https://www.bellingcat.com/news/uk-and-europe/2018/11/16/spies-without-borders-fsb-infiltrated-international-visa-system/ .

Bennett, B., and W. J. Hennigan. 2015. "China and Russia are Using Hacked Data to Target U.S. Spies, Officials Say." *Los Angeles Times*, August 31. http://www.latimes.com/nation/la-na-cyber-spy-20150831-story.html

Bertrand, N. 2015. "Russia and China Could Be 'Making It Impossible for the US to Hide' Its Intelligence Activities." *Business Insider*, September 1. http://uk.businessinsider.com/russia-china-us-intelligence-database-2015-8

Bright, C. 2017. "China to Start Scanning Foreign Travellers' Fingerprints." *Business Insider*, February 10. https://www.businesstraveller.com/destinations/2017/02/10/china-start-scanning-foreign-travellers-fingerprints/

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

Brope, R. "Russia." In *Routledge Companion to Intelligence Studies*, edited by R. Dover, M. S. Goodman, and C. Hillebrand, 227–234. Abingdon: Routledge, 2013.

Callick, R. 2016. "China's All-Seeing Spy Grid Takes Surveillance To New Level." *The Australian*, December 9. http://www.theaustralian.com.au/news/inquirer/chinas-allseeing-spy-grid-takes-surveillance-to-new-level/news-story/7dfdf3fef86da6b8203c6acba3840539

Central Intelligence Agency. 2015. "Deputy Director Cohen Delivers Remarks on CIA of the Future at Cornell University." September 17. 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

CIA. 2011. "CIA Assessment on Surviving Secondary Screening at Airports while Maintaining Cover." September. Published by WikiLeaks, Dec. 21, 2014. https://WikiLeaks.org/cia-travel/secondary-screening/WikiLeaks_CIA_Assessment_on_Surviving_Secondary_Screening.pdf

CIA. 2012. "CIA Advice for US Government Operatives Infiltrating Schengen." January. Published by WikiLeaks, Dec. 21, 2014. https://WikiLeaks.org/cia-travel/infiltrating-schengen/WikiLeaks_CIA_Advice_for_Operatives_Infiltrating_Schengen.pdf

Clark, R. M. *Intelligence Collection*. Washington, DC: Sage, 2014.

CNN. 2017. "Intel Chief Testifies Amid New Russia Revelations." May 23. http://transcripts.cnn.com/TRANSCRIPTS/1705/23/cnr.03.html

Corera, G. 2016. "The Spies of Tomorrow Will Need to Love Data." *Wired*, April 7. http://www.wired.co.uk/article/spies-data-mi6-cia-gordon-corera .

Corera, G. 2018. "Russia 'Sought Access to UK Visa Issuing System'." *BBC News*, November 16. https://www.bbc.co.uk/news/world-europe-46237634

Dorfman, Z. 2018. "Botched CIA Communications System Helped Blow Cover of Chinese Agents." *Foreign Policy*, August 15. https://foreignpolicy.com/2018/08/15/botched-cia-communications-system-helped-blow-cover-chinese-agents-intelligence/

Dorfman, Z., and M. Jenna. 2018. "The CIA's Communications Suffered a Catastrophic Compromise. It Started in Iran." *Yahoo! News*, November 2. https://in.news.yahoo.com/cias-communications-suffered-catastrophic-compromise-started-iran-090018710.html?guccounter=1

Eftimiades, N. *Chinese Intelligence Operations*. Ilford: Naval Institute Press, 1994.

Elder, M. 2013. "Russian Guard Service Reverts to Typewriters after NSA Leaks." *The Guardian*, July 11. https://www.theguardian.com/world/2013/jul/11/russia-reverts-paper-nsa-leaks

The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland. 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." December 3. https://www.rusemb.org.uk/consnews/29 .

Galeotti, M. 2017. "Russian Intelligence Is at (Political) War." *NATO Review*, May 12. http://www.nato.int/docu/review/2017/Also-in-2017/russian-intelligence-political-war-security/EN/index.htm

Garthoff, R. L. *A Journey through the Cold War: A Memoir of Containment and Coexistence*. Washington D.C.: Brookings Institution Press, 2001.

Gioe, D. V. "Handling HERO: Joint Anglo-American Tradecraft in the Case of Oleg Penkovsky." In *An International History of the Cuban Missile Crisis: New Perspectives after Fifty Years*, edited by D. 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, 213–227. London: Palgrave Macmillan, 2017.

Grey, S. *The New Spymasters: Inside Espionage from the Cold War to Global Terror*. London: Penguin Random House, 2015.

Guo, X. *China's Security State: Philosophy, Evolution, and Politics*. Cambridge: Cambridge University Press, 2012.

House of Commons Defence Committee. 2016. "Russia: Implication for UK Defence and Security." March 8. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/russia-implications-for-uk-defence-and-security/oral/30301.html

House of Commons Defence Committee. 2016. "Supplementary Written Evidence Submitted by Dr Victor Madeira." March 25. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/russia-implications-for-uk-defence-and-security/written/31103.pdf

Inkster, N. "Intelligence Agencies and the Cyber World." *Strategic Survey* 112, no. 1 (2012): 33–47. doi:10.1080/04597230.2012.717418.

Inkster, N. "Chinese Intelligence in the Cyber Age." *Survival: Global Politics and Strategy* 55, no. 1 (2013): 45–66. doi:10.1080/00396338.2013.767405.

Institute for Critical Infrastructure. 2015. "Preparing the Battlefield: The Coming Espionage Culture Post OPM Breach." August. https://icitech.org/wp-content/uploads/2015/08/ICIT-Brief-Espionage-Culture-Post-OPM4.pdf .

Jensen, B. M., C. Whyte, and S. Cuomo. "Algorithms at War: The Promise, Peril, and Limits of Artificial Intelligence." *International Studies Review* 22, no. 3 (2020): 526–550. doi:10.1093/isr/viz025.

Jones, S. 2016. "The Spy Who Liked Me: Britain's Changing Secret Service." *The Financial Times*, September 28. https://www.ft.com/content/b239dc22-855c-11e6-a29c-6e7d9515ad15

Kolomychenko, M. 2018. "Russia, Stung by Intelligence Leaks, Plans to Tighten Data Protection." *Reuters*, November 23. https://www.reuters.com/article/us-russia-dataprotection-leaks-idUSKCN1NS0LU

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

Lord, J. "Undercover under Threat: Cover Identity, Clandestine Activity, and Covert Action in the Digital Age." *International Journal of Intelligence and Counterintelligence* 28, no. 4 (2015): 666–691. doi:10.1080/08850607.2015.1022464.

Lucas, E. *Deception: Spies, Lies, and How Russia Dupes the West*. London: Bloomsbury Publishing, 2013.

Lucas, E. *Spycraft Rebooted*. Seattle: Amazon Publishing, 2018.

Lyngaas, S. 2015. "Inside the CIA's New Digital Directorate." *FCW*, October 1. https://fcw.com/Articles/2015/10/01/CIA-digital-directorate.aspx?Page=1 .

Mahmood, S. "Online Social Networks and Terrorism: Threats and Defenses." In *Security and Privacy Preserving in Social Networks*, edited by R. Chbeir and B. A. Bouna. London: Springer, 2013.

Mattis, P. "Beyond Spy Vs. Spy: The Analytic Challenge of Understanding Chinese Intelligence Services." *Studies in Intelligence* 56, no. 3 (2012): 47–57. https://www.cia.gov/resources/csi/studies-in-intelligence/volume-56-no-3/beyond-spy-vs-spy-the-analytic-challenge-of-understanding-chinese-intelligence-services/ .

McFarland, M. 2017. "146,000 Cameras Monitor Moscow Streets. And the Government Is Just Getting Started." *CNN*, June 14. http://money.cnn.com/2017/06/14/technology/culture/moscow-cameras/index.html

McLaughlin, J., and Z. Dorfman. 2018. "At the CIA, a Fix to Communications System that Left Trail of Dead Agents Remains Elusive." *Huffington Post*, June 12. https://www.huffingtonpost.com/entry/at-the-cia-a-fix-to-communications-system-that-left-trail-of-dead-agents-remains-elusive_us_5c094117e4b069028dc7696a

Mendez, A. J., and M. Malcolm. *The Master of Disguise: My Secret Life in the CIA*. London: Harper Collins, 2007.

Mendez, A. J., J. Mendez, and M. Baglio. *The Moscow Rules: The Secret CIA Tactics that Helped America Win the Cold War*. New York: Public Affairs, 2019.

Miller, G. 2016. "As Russia Reasserts Itself, U.S. Intelligence Agencies Focus Anew on the Kremlin." *The Washington Post*, September 14. 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?utm_term=.d969a442ac3a82 .

Miller, G. 2016. "Moscow Rules of Espionage Go Global – If You Think Its KGB, It Is." *Observer*, June 30. http://observer.com/2016/06/moscow-rules-of-espionage-go-global-if-you-think-its-kgb-it-is/ .

Mo, Z. 2017. "Fingerprinting Of Foreign Visitors Gets Started At Shenzhen's Bao'an Airport." *China Daily*, November 2. http://www.chinadaily.com.cn/china/2017-02/11/content_28168119.htm

Morris, H. 2017. "Russia Wants to See Your Salary and Social Media Accounts before Letting You Visit." *The Telegraph*, July 21. https://www.telegraph.co.uk/travel/destinations/europe/russia/articles/russia-introduces-social-media-visa-application/

Mosbergen, D. 2019. "Nearly All U.S. Visa Applicants Now Required to Submit 5-Year Social Media History." *Huffington Post*, June 3. https://www.huffingtonpost.co.uk/entry/visa-social-media-state-department_n_5cf4898ce4b0e8085e3bfde1?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAImALRHTwaQyk9Lu3BCqYlCdJjsHnXXur6Gu-UCvjyknbwpH-hjDYnM_5gsx3zeIhVO05YVF_migMkIpe3CyyQvPSHXaituIb3iLew56P8YH3_0i40dTZkT3LVrkSRhauyRuNwT_MGWfP4c8tkQaeWpPkDnKyAr0a1ANiCQdflqo

Mozur, P. 2018. "Inside China's Dystopian Dreams: A.I, Shame and Lots of Cameras." *The New York Times*, July 8. https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html

Murphy, J. 2015. "How Technology Is Changing the Future of Espionage." *Sofrep*, March 24. https://sofrep.com/40315/technology-changing-future-espionage/

Nakashima, E. 2015. "With a Series of Major Hacks, China Builds a Database on Americans." *The Washington Post*, June 5. 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

Official Internet Resources of the President of Russia. 2017. "Meeting of Federal Security Service Board." February 16. http://en.kremlin.ru/events/president/news/53883

Olson, J. M. "A Never-ending Necessity: The Ten Commandments of Counterintelligence." *Studies in Intelligence* 11 (2001): 81–87.

Osborne, H., and S. Cutler. 2019. "Chinese Border Guards Put Secret Surveillance App On Tourists' Phones." *The Guardian*, July 2. https://www.theguardian.com/world/2019/jul/02/chinese-border-guards-surveillance-app-tourists-phones

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

Philipp, J. 2016. "You're on File: Exclusive inside Story on China's Database of Americans." *Epoch Times*, March 1. https://www.theepochtimes.com/youre-on-file-exclusive-inside-story-on-chinas-database-of-americans_1973047.html

Rogin, J. 2016. "Russia Is Harassing U.S. Diplomats All Over Europe." *The Washington Post*, June 26. 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

Rohde, D. 2016. "Special Report – John Brennan's Attempt to Lead the CIA into the Age of Cyberwar." *Reuters*, November 2. 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

Royden, B. G. "Tolkachev, a Worthy Successor to Penkovsky." *Studies in Intelligence* 47, no. 3 (2003). https://www.cia.gov/resources/csi/studies-in-intelligence/archives/vol-47-no-3/tolkachev-a-worthy-successor-to-penkovsky/ .

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

Ryzhkov, V. 2014. "Controlling Russians through Travel Bans." *The Moscow Times*, May 16. https://themoscowtimes.com/articles/controlling-russians-through-travel-bans-35830

Sanger, D. E., and E. Schmitt. 2014. "Snowden Used Low-Cost Tool to Best N.S.A." *The New York Times*, February 9. https://www.nytimes.com/2014/02/09/us/snowden-used-low-cost-tool-to-best-nsa.html?hp&_r=1

Sano, J. R. "The Changing Shape of HUMINT." *Intelligencer* 21, no. 3 (2015): 77–80.

Security Magazine. 2019. "China Cracking down on Data Theft Caused by Mobile Apps." August 16. https://www.securitymagazine.com/articles/90732-china-cracking-down-on-data-theft-caused-by-mobile-apps

Shane, S., M. Rosenberg, and A. W. Lehren. 2017. "Wikileaks Releases Trove of Alleged C.I.A. Hacking Documents." *The New York Times*, March 7. https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html

Shulsky, A. N., and G. J. Schmitt. *Silent Warfare: Understanding the World of Intelligence*. Washington, DC and London: Brassey's, 2002.

Slick, S. 2016. "Measuring Change at the CIA." *Foreign Policy*, May 4. http://foreignpolicy.com/2016/05/04/measuring-change-at-the-cia/ .

Soldatov, A., and I. Borogan. *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB*. New York: Public Affairs, 2010.

Soldatov, A., and I. Borogan. 2011. "A Face in the Crowd: The FSB Is Watching You!" *openDemocracy*, November 15. https://www.opendemocracy.net/od-russia/andrei-soldatov-irina-borogan/face-in-crowd-fsb-is-watching-you

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.

Stein, J. 2012. "CIA's Secret Fear: High-Tech Border Checks Will Blow Spies' Cover." *Wired*, December 4. https://www.wired.com/2012/04/cia-spies-biometric-tech/

Stein, J. 2017. "Chinese Counterspies Roiling U.S. Intelligence Operations in Beijing." *Newsweek*, May 22. http://www.newsweek.com/chinese-counterspies-roiling-us-intelligence-operations-613393

Stone Fish, I. 2015. "Why Can't Ex-Chinese Leaders Travel Abroad." *Foreign Policy*, December 24. https://foreignpolicy.com/2015/12/24/why-are-former-chinese-leaders-prevented-from-traveling-overseas-xi-jinping/

Stratfor Global Intelligence. 2010. "Intelligence Services, Part 1: Espionage with Chinese Characteristics." March. Published by WikiLeaks. https://WikiLeaks.org/gifiles/attach/133/133464_INTEL_SERVICES_CHINA.pdf

Streeter, D. 2013. "Biometrics and Intelligence Asset Protection: Biometric Technology and Its Impact on Counterintelligence and Intelligence." Unpublished paper written at Liberty University Helm's School of Government.

Syeed, N. 2016. "CIA Cyber Official Sees Data Flood as Both Godsend and Danger." *Bloomberg*, August 1. https://www.bloomberg.com/news/articles/2016-08-01/cia-cyber-official-sees-data-flood-as-both-godsend-and-danger

Tatlow, D. K. 2014. "China Approves Security Law Emphasizing Counterespionage." *New York Times*, November 2. https://www.nytimes.com/2014/11/03/world/asia/china-approves-security-law-emphasizing-counterespionage.html?ref=asia

Teabeamet (Estonian Information Board). 2017. "International Security and Estonia". https://www.valisluureamet.ee/pdf/2017-en-c482143c.pdf

Trump White House Archives. 2017. "National Security Strategy of the United States of America." December. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf .

Tucker, D. *The End of Intelligence: Espionage and State Power in the Information Age*. Stanford: Stanford University Press, 2014.

Tucker, P. 2015. "CIA Restructuring Adds New Cyber Focus." *Defense One*, March 6. http://www.defenseone.com/technology/2015/03/cia-restructuring-adds-new-cyber-focus/106953/

Urban, M. 2016. "MI6 Set to Recruit 1,000 Extra Staff." *BBC News*, September 21. http://www.bbc.co.uk/news/uk-37434131 .

Walker, S. 2016. "Face Recognition App Taking Russia by Storm May Bring End to Public Anonymity." *The Guardian*, May 17. https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte

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

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

Watkins, A. 2017. "Russia Escalates Spy Games after Years of US Neglect." *Politico*, June 1. https://www.politico.eu/article/russia-escalates-spy-games-after-years-of-us-neglect/

Yin, C. 2015. "More 'Eyes' Fight Crime in Crowds." *China Daily*, March 10. http://www.chinadaily.com.cn/china/2015-10/05/content_22091634.htm

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

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

Zhumatov, S. 2020. "Russia Expands Facial Recognition Despite Privacy Concerns." *Human Rights Watch*, October 2. https://www.hrw.org/news/2020/10/02/russia-expands-facial-recognition-despite-privacy-concerns