Shape or Deter? Managing Cyber-Espionage Threats to National Security Interests

Lester Godefrey

Opting out of cyber espionage places modern intelligence collection organizations at a strategic disadvantage; by not participating, they would inevitably miss out on intelligence that is difficult if not impossible to collect using existing traditional means.

In this article, the first of its kind in Studies*, a UK government analyst argues that cyber espionage is the natural evolution of intelligence gathering statecraft in the 21st century. He explores whether deterrence by denial or punishment is likely to be successful in significantly reducing or preventing cyber espionage against national security interests. Using open-source materials for his case study, he considers whether US efforts to counter cyber espionage by China have achieved deterrence or reduced activity.*

In addition to the caveats that apply to every Studies *article, the author's statements should not be construed as the endorsement by or official judgments of any component of Her Majesty's Government.*

Introduction

Espionage is a fundamental tool of statecraft. In existence since the formation of organized societies, the modern era of nation states has codified and institutionalized the profession and tasked it with the theft of secrets at industrial scale.[1] As societies move overwhelming to storing data digitally in networked environments, cyber espionage is a natural evolution for intelligence agencies required to steal secrets. For intelligence agencies to deliver the supply of intelligence that their governments demand, spies must conduct cyber espionage.

Furthermore, the cost of standing up new cyber espionage capabilities is rapidly decreasing due to the proliferation of tooling and expertise in both licit and illicit marketplaces. Opting out of cyber espionage places modern intelligence collection organizations at a strategic disadvantage; by not participating, they would inevitably miss out on intelligence that is difficult if not impossible to collect using existing traditional means such as signals intelligence (SIGINT) or human intelligence (HUMINT).

Abstaining from cyber espionage also reduces intelligence agencies' visibility and ability to counter-detect foreign espionage against their own interests. As intelligence agencies develop and mature in the 21st century, cyber espionage is highly likely to be (if not already) an operational necessity. Intelligence agencies cannot be deterred into opting out without risking their ability to fulfill their mandate. The norms and behaviors of cyber espionage can, however, be shaped by government action. Counterintelligence theorists and practitioners have long advocated shaping operations toward hostile espionage operations by disregarding the pretense that espionage can be significantly reduced or wholly

Incorporating diplomatic engagement into shaping operations also provides governments with the ability to signal clear expectations of norms and behavior when conducting cyber espionage.

deterred. Instead, their goals are to detect and manipulate espionage activities through a range of overt and clandestine measures.[2]

Using shaping operations to apply operational pressure to competitors and adversaries carrying out cyber intrusions is highly complementary to the strategy of "persistent engagement," a doctrinal concept defined by US Cyber Command as "continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver."[3] Identifying hostile cyber-espionage operations and degrading their technical and operational capabilities through exposure, deception, and disruption are entirely consistent with existing counterintelligence approaches and practices.

Incorporating diplomatic engagement with competitor and adversary nations into shaping operations also provides governments with the ability to signal clear expectations of norms and behavior when conducting cyber espionage. For example, a cyber-espionage operation against a government's military network could be signaled as undesirable but expected, whereas an espionage operation against a virology lab to steal test data could be communicated as intolerable and an escalation trigger.

It is highly unlikely that cyber espionage as a practice will end before networked societies end. As a result, counter-cyber-espionage programs must settle in for the long haul.

Definitions and Challenges

One of the biggest challenges in the academic study of cyber operations is the difficulty in agreeing on definitions, making it essential to spell them out. This article utilizes the *Oxford Bibliographies* definition of cyber espionage as "the exploitation of cyberspace for the purpose of accessing and collecting confidential data".[4]

Cyber espionage is typically carried out either by state organizations, such as intelligence agencies, or by non-state actors tasked or co-opted by states; these can include contractors, cyber criminals, and private companies. Threat actors involved in cyber espionage can use a range of computer network exploitation (CNE) techniques to gain access to networks and devices, including spear phishing, vulnerability exploitation, and supply chain compromise.[5]

A challenge for network defenders is distinguishing the intent of threat actors; for example, a threat actor gaining access to a defense manufacturer's network may be attempting to steal data for espionage purposes. Alternatively, they may be attempting to create offensive cyber technical effects on defense platforms (computer network attack, or CNA), or creating access for future offensive exploitation (operational preparation of the environment, or OPE).[6] Assessing threat-actor intent is a continuous challenge for defenders who will always have imperfect insights.

The challenge of distinguishing intent also contributes to the frequent equivocation of cyber espionage with cyber attacks, i.e., incidents where devices, data, or networks are subject to disruption, denial, degradation, or destruction effects.[7] However, this term is often stretched to include any intrusion or data theft.

This conflation is especially common in public policy. For example, the compromise in 2015 of the US Office for Personnel Management (OPM)'s security clearance database was widely described by policymakers as a cyber attack, despite US intelligence officials publicly identifying the intrusion as espionage by threat actors intent on stealing personal identifiable information (PII) of security-cleared personnel.[8] [9]

Espionage Norms

Espionage is largely uncodified in international law. Instead, it is governed by explicit and implicit norms within the international system.[a] It is an expected and largely accepted aspect of international relations; while there is a lack of consensus amongst international law scholars over whether espionage between states is lawful, there is no dispute that it is a major feature of the system.[10] Espionage typically violates the domestic law of the country being targeted, while states that engage in espionage will also often (although

a. Borrowing from just war theory and the criteria of *jus in bello*, or right conduct in war, some ethics scholars argue intelligence is principally an epistemic activity governed by the principles of discrimination, necessity, proportionality, and reciprocity.

not always) enact statutes that legalizes and codifies its practice.

States largely accept and acknowledge that the Vienna Convention on Diplomatic Relations is routinely utilized by countries to place intelligence officers in their embassies under diplomatic official cover. Intelligence officers can also use non-official cover to infiltrate countries under false pretences, thus violating domestic immigration laws. States can shape intelligence activities by expelling spies working under diplomatic cover by declaring them *persona non grata*, often with the expectation of proportional retaliation. Similarly, intelligence officers and agents that are caught and imprisoned can be exchanged between countries in "spy swaps," as in the reported exchange of alleged Russian, US, and British intelligence agents and officers in 2010.[11]

There is a lack, however, of publicly avowed diplomatic treaties and agreements between states on espionage, meaning normative concepts are blurry at best. Attempted assassinations of spies are a significant point of dispute. The attempted murder in 2018 of Sergei Skripal by GRU officers using a chemical weapon in the UK violated the UN Charter and Russia's obligations under the Chemical Weapons Convention.[12] It is much less clear as to whether the attempted assassination was a violation of an implicit convention in espionage not to kill defectors exchanged in spy swaps.[13] [14]

The fluidity and opacity of norms in international espionage, combined with lack of international legal frameworks and oversight, make it a challenge to influence state behavior. States largely regard espionage as a vital tool of statecraft and often only attempt to constrain it in line with national policy objectives. To prohibit, for instance, the intercept of heads of states' private emails would most likely require an international treaty outlawing the process and a mandated dispute-resolution process, with meaningful penalties for noncompliance.

The fluidity and opacity of norms in international espionage and lack of international legal frameworks make it a challenge to influence state behavior.

The creation of such mechanisms, however, is extremely unlikely. Just as states have historically shown little desire to limit the means by which they pursue intelligence, so too have they thus far shown little appetite to constrain their cyber capabilities, and there remains widespread disagreement as to how international law applies to cyberspace.[15] The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*[a] concludes that cyber espionage as a practice generally does not violate international law, though the methods used in cyber espionage might rise to unlawful under certain conditions.[16]

Deterrence or Shaping?

Policy documents and academia tend to blur the distinctions of deterrence and shaping activities. The UK Ministry of Defence (MOD) *Joint Doctrine Note 1/19* defines deterrence as "the aim to dissuade a course of action." Restrictive deterrence defines acts that take place against UK interests that are "undesirable" that the UK "wishes to deter" but cannot realistically do so without imposing unacceptable costs on the UK. *Note 1/19* signposts espionage and cyber attacks as potential examples of this, while noting that certain acts may necessitate "absolute deterrence: deterring something so completely unacceptable that it cannot be allowed to happen under any circumstances."[17]

Alex Orleans, an analyst at cybersecurity provider CrowdStrike, argues that when policy advocates invoke deterrence in contemporary national security policymaking, they often do so with a connotation of that "absolute deterrence"—especially via punishment—and that connotation itself arising from the manner in which nuclear deterrence was discussed during the Cold War. As such, when officials talk of deterring cyber intrusions, including those for the purposes of espionage, it can create a false impression that cyber-espionage activity can be reduced or eliminated entirely through deterrence.[18]

Lithuanian defense adviser Vytautas Keršanskas provides a useful model for defining response thresholds for deterring "hybrid threats," such as influence operations and covert action. In his proposal, "tolerable hostile activities" that do not rise to the threshold of intolerable are best countered with deterrence by denying the benefits of hostile activities to adversaries and increasing defenders' overall resilience.

a. The *Tallinn Manual* is produced by the NATO Cooperative Cyber Defence Centre of Excellence and is widely regarded as the definitive reference work on how international law applies to cyber operations.

Using the model for cyber espionage risks treating intelligence collection and influence operations on a sliding scale when their very purposes are different by design.

Once activities tip into intolerable means or levels, then differentiated responses can be engaged that focus on deterrence by punishment. Keršanskas also advises not to give adversaries exact details on tolerance thresholds for hostile activities, for fear that they may exploit these boundaries to minimize pushback.[19] This, however, raises a fundamental contradiction: how can we expect to deter cyber intrusions when we cannot communicate to our adversaries clear thresholds for their activities, and our proportionate response? While this model offers obvious benefits for quantifying threshold hostile activities and the relative weight of countermeasures, it is designed for measure blended clandestine, covert and overt state activities designed to project geopolitical power, not "passive" intelligence collection.

Using the model for cyber espionage risks treating intelligence collection and influence operations on a sliding scale when their very purposes are different by design. Distinguishing intelligence collection activities in cyberspace, i.e., cyber espionage, from influence operations or covert action is challenging but should be a key objective of any analytical framework designed to influence hostile cyber operations.

Instead, cyber-espionage activities are ideal candidates for "shaping operations." In UK *Allied Joint Doctrine Publication 5-00*, shaping is defined as "the manipulation of the operational environment to the acting organisation's advantage and to the disadvantage of an adversary." Shaping includes identifying areas where the defender's strengths can be exploited while seeking to minimize the adversary's strengths.[20]

Although *5-00* calls out deterrence as a potential positive effect, it is not the ultimate objective of shaping operations; instead, shaping seeks to give defenders advantages and competitors disadvantages. If we take the view that cyber espionage is a natural and inevitable component of intelligence gathering in networked societies, our methods must reflect this. Deterrence should be reserved for preventing the intolerable, while shaping focused on the undesirable but inevitable. In this regard, shaping operations represent a uniquely suitable approach to degrading adversary cyber operations in keeping with both traditional counterintelligence theory and the particular dynamics of cyber intrusions.

Case Study: US Response to China's State-Sponsored Cyber Espionage, 2000–20

In 2005, US media reported that a cyber-espionage intrusion set known as *Titan Rain* targeting the US government and defense industrial base had been attributed to the People's Liberation Army (PLA).[21] [22] US government identification and response to PRC-attributed cyber-espionage campaigns remained largely nonpublic until the identification of the Operation *Aurora* campaign, which primarily targeted the US high-tech and defense sectors. Many of the campaign's publicly reported goals remained consistent with intelligence gathering, including the purported targeting of Gmail's lawful-intercept monitoring system to identify which accounts were subject to US FISA warrants.[23]

In addition to classic intelligence collection, the theft of commercially sensitive intellectual property (IP) from companies targeted in Operation *Aurora*, including proprietary source code used in commercial programs, heighted policymaker scrutiny of China's cyber espionage. *Aurora* correlated with existing lawmaker concerns that Beijing's cyber-espionage campaigns were stealing IP for the commercial benefit of Chinese companies. In October 2011, the US Director of National Intelligence (DNI) said in an unclassified report to Congress that cyber espionage originating from China resulting in IP theft was a growing problem.[24]

The public evidence indicates that after Operation *Aurora*, the Obama administration began a policy of public and private engagement with Beijing to shape, rather than deter, PRC cyber-espionage activities. The purpose of the strategy was to persuade PRC leadership that ongoing cyber-espionage activities against the US were unpleasant but tolerable, while Chinese cyber-espionage units stealing IP for the benefit of Chinese commerce was intolerable and would damage bilateral relations. This engagement culminated in 2015 with the US-China Cyber Agreement, which included a pledge not to engage in cyber espionage for the purposes of commercial gain.[25]

In February 2013, the cybersecurity firm Mandiant publicly released a report which attributed the APT1 cyber espionage group to PLA Unit 61398 with high confidence. The

report alleged that the group steals "broad categories of intellectual property" for the likely benefit of Chinese industries.[26] More than a year later, The US Department of Justice (DOJ) followed suit with criminal charges against several Unit 61398 personnel for both computer theft and economic espionage, naming several US private firms as victims.

The US strategy seemed clearly aimed at dissuading the PRC government from engaging in IP theft using cyber means first and foremost, rather than intelligence gathering using cyber means. Then Chairman of the Joint Chiefs of Staff General Martin Dempsey commented publicly in 2013 that he was engaging with PLA leaders "establish some rules of the road" in cyber operations, specifically touching on IP theft.[27]

Partial Success

Judged solely on publicly available information, this strategy of public-private engagement and coercion is likely to have been only partly successful. While private-sector data indicate that PRC cyber-espionage campaigns against the private sector dipped significantly before and after the signing of the 2015 Obama-Xi agreement, this probably reflects a publicly reported reorganization and rationalization of PRC cyber-espionage units drawn from the PLA and the Ministry of State Security (MSS).[28] [29]

China's cyber-enabled economic espionage has continued, although it can now be viewed at least partially through the lens of industrial strategy goals like the "Made in China 2025" 10-year plan. The strategy calls on both state and private sector entities to rapidly acquire and develop key technologies critical for China's economic growth, such as semiconductor fabrication and aviation turbofans.[30]

Beijing's strategy calls on both state and private sector entities to rapidly acquire and develop key technologies critical for China's economic development.

One interpretation that might explain PRC leadership directing the continuation of economic espionage while claiming not to renege on the Xi-Obama agreement is directives like "Made in China 2025" are for national benefit, rather than the private financial benefit of commerce. This case study demonstrates how strategies of engagement are never guaranteed to lead to mutual understanding in international relations.

Beyond the agreement, the US government has been inconsistent in its public statements directed toward the PRC on the issue of cyber espionage. The Office of Personnel Management (OPM) had personnel records for least 4 million federal employees stolen in 2014 by a cyber espionage group allegedly based in China.[31] Top US intelligence officials publicly indicated the gravity of the intrusion for US national security interests but played down the incident as a hostile action by China. DNI James Clapper went as far to say that "you have to kind of salute the Chinese for what they did... If we had the opportunity to do that [to them], I don't think we'd hesitate for a minute."[32]

Then director of the National Security Agency, Adm. Mike Rogers, testified to Congress that the intrusion was not a cyber attack, reinforcing Clapper's definition of the breach as "passive intelligence collection activity—just as we do."[33] As part of a deliberate shaping strategy, this could be interpreted as a signal to PRC officials as the tacit acceptance of legitimate, if undesirable, cyber espionage for the purposes of intelligence collection, especially in contrast to strong US denunciations of cyber-enabled IP theft.

In comparison, White House officials and many elected members of Congress often refused to acknowledge this distinction, calling for direct reprisals against Beijing to deter breaches of this scale.[34] This surely undermined the consistency of the message heard by PRC leadership that their activities were unwelcome but within the scope of intelligence norms.

Blurred Lines

Post-2015 US criminal indictments of hackers allegedly employed by PRC intelligence have also potentially blurred previously made distinctions that cyber espionage for traditional intelligence gathering is legitimate but economic espionage against private businesses is not. Breaches of US financial services, health care, and hospitality firms that US intelligence agencies publicly assessed were "passive intelligence collection activity" of PII were condemned by US government officials as unacceptable breaches of US citizens' privacy, for which PRC hackers would be found criminally culpable.

Several hackers allegedly employed by the PLA were indicted in 2020 for their purported theft of PII pertaining to 145 million Americans from Equifax credit services in 2017. Journalist Zach Dorfman reported that bulk PII collection by PRC

Conflating economic crime and intelligence gathering in criminal charges brought against PRC-sponsored hackers has muddied the waters.

intelligence units may have been for the purposes of counterintelligence, in order to identify US intelligence officers and security-cleared personnel.[35]

Public statements by then Attorney General William Barr indicated that the indictment was in response to "the disturbing and unacceptable pattern of state-sponsored computer intrusions and thefts by China and its citizens that have targeted personally identifiable information, trade secrets, and other confidential information."[36] The US government now appeared to be signaling to the Chinese government that PII belonging to US citizens was now similarly off limits, as well as IP.

Indictments now began to criminalize Chinese hackers for their involvement in conventional espionage as well. In 2018, the DOJ unsealed charges against two hackers associated with APT10, a contractor group allegedly employed by the MSS. The indictment charged the hackers with breaking into a US Navy personnel database, in addition to IP theft campaigns against the private sector.[37] Similarly, in 2020 APT41 were indicted for cyber-espionage operations against several foreign governments, including the United Kingdom. [38]

The DOJ policy shift from targeting criminal indictments primarily against Chinese hackers associated with IP theft to espionage and cybercrimes more broadly may be explainable as consistent with the Trump administration's promise to "get tough on China" and issue more indictments against PRC intelligence. In a 2018 speech on Chinese economic espionage, Attorney General Jeff Sessions alleged that between 2013 and 2016 the Obama administration "did not charge anyone with spying for China," while the DOJ under his leadership had charged three people for espionage in the first year of the Trump administration.[39]

Criminal indictments can be used to disrupt activities as much as to criminally sanction perpetrators, and publicly attributing responsibilitity can force changes in tactics, techniques, and procedures. Conflating economic crime and intelligence gathering in criminal charges brought against PRC-sponsored hackers, however, has muddied the waters. Does the US seek to deter cyber espionage by the PRC government as a whole or shape it to prevent the most egregious and disruptive behaviors? Beijing could counter that Washington does not accept its right to carry out cyber espionage as part of legitimate statecraft, and so all previous attempts at signaling can be dismissed as insincere bluster.

While the combination of economic sanctions, criminal indictments and diplomatic engagement are likely to have influenced targeting and operational security decisions by PRC intelligence actors, we lack data to argue that these engagements can meet any known criteria of preventing espionage. Indeed, it is unclear to an outsider what US policy goals of deterrence were at all due to the lack of continuity over the decade.

Shaping Operations in Cyber Espionage

The frequent difficulty in differentiating between deterrence and shaping activities toward cyber espionage—what activities are undesirable but acceptable, versus those which are intolerable—has led to opaqueness in both communicating expectations to adversaries and setting national objectives toward adversary cyber espionage. These tensions were visible in the joint Five Eyes statement in April 2021 that attributed the SolarWinds supply chain compromise to APT29, a threat group linked in open sources to Russia's foreign intelligence agency, the SVR.

Both the UK and US publicly issued intelligence assessments that the SolarWinds initial compromise and follow-on intrusion activities were most likely for the purpose of intelligence collection, rather than CNA or OPE. At the same time, the decision to make the attribution public was justified as a response to the scale of the Russian cyber operation against SolarWinds customers, packaged with both additional denouncement of Russian electoral interference activities and targeted sanctions against Russian government and private sector entities.

A US Treasury press release stated the "scope and scale of this compromise combined with Russia's history of carrying out reckless and disruptive cyber operations makes it a national security concern."[40] The UK Foreign Office's official statement on SolarWinds characterized the cyber espionage campaign as "malign behavior" that was part of a wider pattern of "election interference and aggressive behavior."[41]

Condemnation of SolarWinds as malign leaves Five Eyes members open to charges of hypocrisy. Thomas Rid, an expert on cyber and information operations practices, argues that the sanctions package did not resolve "how was SolarWinds different from high-end Five Eyes intelligence operations?"[42] Former CIA intelligence officer Paul Kolbe concurred, arguing that the US is "engaged in the same type of operations at an even grander scale."[43]

J. Michael Daniel, president of the Cyber Threat Alliance and a former White House official, suggests the scale and disproportionality of the SolarWinds initial access campaign made it worth singling out as a violation of cyber-espionage norms worthy of economic sanctions. This, however, raises the same questions as the White House's reported response to the OPM breach, which called for retaliation on grounds of scale (or in *jus in bello* terms, proportionality). As such, it does not appear that scale of operations has been a useful rubric for determining deterrence thresholds. The justifications for diplomatic denunciations and sanctions could be much clearer in distinguishing the SolarWinds campaign and why it demands an escalatory response.[44]

Public attribution of APT29 has tangible benefits for national cyber defense through imposing costs on adversaries and increasing private sector awareness of cyber-espionage threats. Characterizing hostile cyber operations by adversaries on the one hand as intelligence collection and on the other as "undermining democracy" risks confusing both defenders and adversaries. The UK has clearly distinguished in previous cases that it does differentiate between hostile intelligence operations against the UK and egregiously harmful covert actions against UK interests, such as electoral interference and attempted assassinations. The blurred lines of cyber operations have at times made distinguishing these activities harder.

In today's networked societies and economies, cyber espionage is the natural evolution of modern intelligence practices.

Essential Statecraft

I have argued that it is not realistic to expect that nation-states can deter cyber-espionage activities against its national interests; intelligence collection is too established as part of the framework of modern statecraft and no tools exist that can reliably prevent it, although counterintelligence as a discipline is intended to at least frustrate it. In today's networked societies and economies, cyber espionage is the natural evolution of modern intelligence practices. So far as the social conditions exist, states will seek to utilize it.

Shaping cyber espionage by creating friction, imposing costs, and signaling is a much more accurate reflection of both existing counterintelligence practices and achievable goals. Framing disruption activities against cyber espionage as shaping operations also helps suggest potential strategies with realistic goals. We cannot prevent it, but we can make it harder and less successful.

Some potential policy goals derived from a shaping framework include:

- A focus on identifying the behaviors in cyber-espionage activities most likely to cause inadvertent or uncontrolled escalation;
- Identifying and preventing IP theft carried out by state intelligence agencies for private commercial gain;
- Preventing cyber-espionage operations that are most likely to damage critical national infrastructure (for instance, electricity generation or water treatment facilities);
- Prioritizing overt disruption, such as legal sanctions regimes, for cyber-espionage activities that are assessed to violate espionage norms.

Under this framework, governments could consider a variety of options. These include developing a government-wide matrix of unacceptable behaviors by cyber-espionage actors that would trigger an elevated counterintelligence/disruption response. States could use public and private communication channels to signal acceptable and unacceptable behavior. Similarly, states could use offensive (destructive) cyber capabilities to disrupt an adversary's intelligence operations and infrastructure.

Several of these recommendations are likely to be highly challenging and would require extensive policy development before utilization. For example, developing hard categorisations of unacceptable behaviors in cyber operations and communicating them to adversaries can create opportunities for threat actors to operate just under escalation thresholds. Perri Adams and others have suggested several aspirational norms for "responsible offensive cyber operations"

Clarifying goals to shape, rather than deter, foreign cyber espionage would help define realistic expectations of what nation-states and their allies can achieve.

(such as avoiding indiscriminate targeting and predeployment testing of CNE capabilities), rather than negative norms to score against when violations are identified.[45]

Conclusion

More public research is required on which behaviors in cyber operations are the most likely to trigger escalation when identified by a defender. For example, observers can right now only speculate as to what the response might be from a detected intrusion into US strategic nuclear command and control networks by a cyber-threat actor, especially if the intent of the operation is vague. However, these recommendations offer the opportunity to influence and mitigate the negative consequences of one of the greatest expansions in intelligence collection since the invention of the telegraph. We cannot stop or reverse cyber espionage and we would be foolish to try; however, we must not cede our responsibilities to influence and govern it for the benefit of Five Eyes national security.

There are distinct benefits of adopting a strategy that provides partners and adversaries clear direction on how we can influence cyber-espionage norms and behaviors. Clarifying goals to shape, rather than deter, foreign cyber espionage against national interests would help define realistic expectations of what nation-states and their allies can achieve against competitors and adversaries, while helping to prevent inadvertent escalation in international relations. In sum, while there is little to gain and significant costs in seeking to deter cyber espionage, seeking to shape it offers both a much more grounded view of what can be achieved within existing operational constraints and helps expand our viewpoint of what is possible.

❖ ❖ ❖

The author: Lester Godefrey is the pen name of a UK government analyst.

Endnotes

1. Adam Sisman, "Christopher Andrew's history of spying shows how undercover ops have changed history," *New Statesman,* www.newstatesman.com/culture/books/2018/08/christopher-andrew-s-history-spying-shows-how-undercover-ops-have-changed.
2. William Johnson, *Thwarting Enemies at Home and Abroad* (Georgetown University Press, 1987).
3. Jacquelyn Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," *Lawfare,* https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy.
4. Russell Buchan, Iñaki Navarrete, "Cyber Espionage," *Oxford Bibliographies*, 2020, https://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0212.xml.
5. MITRE, MITRE ATTACK Tactics Enterprise: Initial Access, www.attack.mitre.org/tactics/TA0001/.
6. Ministry of Defence (UK), "Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities," https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf.
7. Matthew Monte, *Network Attacks and Exploitation: A Framework* (Wiley, 2015).
8. Partricia Zengerle, "US senators say OPM data breach appears state-sponsored." Reuters, www.reuters.com/article/us-cybersecurity-usa-congress-idUSKBN0OQ1YD20150610.
9. Michael Adams, "Why the OPM Hack Is Far Worse Than You Imagine," *Lawfare,* www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.
10. John A. Radsan, "The Unresolved Equation of Espionage and International Law," *Michigan Journal of International Law,* 596–623, www.repository.law.umich.edu/cgi/viewcontent.cgi?article=1170&context=mjil.
11. *BBC News*, "Spies swapped by US and Russia at Vienna airport," www.bbc.co.uk/news/10564994.
12. *UN News*, "UK letter to Security Council says 'highly likely' Russia behind nerve-agent attack; Russia denies responsibility." www.news.un.org/en/story/2018/03/1005272.
13. Ewan MacAskill, "Has the cold war idea of 'spy etiquette' disappeared?" *The Guardian,* www.theguardian.com/world/2018/mar/09/cold-war-spy-etiquette-poisoning-sergei-skripal.
14. Michael Schwirtz, Jose Bautista, "Poisoned Russian Ex-Spy Is Said to Have Worked With Spanish Intelligence," *New York Times*, https://www.nytimes.com/2018/09/06/world/europe/skripal-poison-russia-spy-spain.html.
15. Harriet Moynihan, "The Application of International Law to State Cyberattacks," Chatham House, www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/2-application-sovereignty-cyberspace.
16. CCDOE, "Tallinn Manual 2.0: Cyber Espionage Generally Not Unlawful," https://ccdcoe.org/news/2017/tallinn-manual-2-0-cyber-espionage-generally-not-unlawful/.
17. Ministry of Defence (UK), "Joint Doctrine Note 1/19: Deterrence: the Defence Contribution," https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/860499/20190204-doctrine_uk_deterrence_jdn_1_19.pdf.
18. Alex Orleans, "The Incoherence of Cyber Deterrence," *Horkos*, https://horkos.medium.com/the-incoherence-of-cyber-deterrence-c78253372eb1.
19. Vytautus Keršanskas, "Deterrence: Proposing a more strategic approach to countering hybrid threats," *Hybrid CoE,* www.hybridcoe.fi/wp-content/uploads/2020/03/Deterrence.pdf.
20. Ministry of Defence (UK), *Joint Doctrine Publication 5-00*, http://www.defencesynergia.co.uk/wp-content/uploads/2016/08/NATO-Allied-Joint-Doctrine-for-Operational-level-planning-with-UK-elements-2013.pdf.
21. Nathan Thornburgh, "The Invasion of the Chinese Cyberspies." *Time*, http://content.time.com/time/subscriber/article/0,33009,1098961,00.html.
22. Bradley Graham, "Hackers Attack Via Chinese Web Sites," *Washington Post*, www.washingtonpost.com/archive/politics/2005/08/25/hackers-attack-via-chinese-web-sites/03559eb7-4e56-40bf-b406-8198bd1e1131/
23. Ariana Eunjung Cha, Ellen Nakashima, "Google China cyberattack part of vast espionage campaign, experts say," *Washington Post*, www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html.
24. Director of National Intelligence, "Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011," www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf.
25. Congressional Research Service. 2015. "US-China Cyber Agreement," https://fas.org/sgp/crs/row/IN10376.pdf.
26. Mandiant, "APT1: Exposing One of China's Cyber Units," www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.
27. Peter Singer, "Defending the nation at network speed: A discussion on cybersecurity with General Martin E. Dempsey, US Army," Brookings Institution, www.brookings.edu/wp-content/uploads/2013/06/20130627_dempsey_cybersecurity_transcript.pdf.
28. FireEye iSIGHT Intelligence, "Red Line Drawn: China Recalculates Its Use of Cyber Espionage," www.fireeye.com/blog/threat-research/2016/06/red-line-drawn-china-espionage.html.

29. Elsa B. Kania, John K. Costello "The Strategic Support Force and the Future of Chinese Information Operations." Cyber Defense Review (Spring 2018). http://web.archive.org/web/20210505193148/https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Strategic%20Support%20Force_Kania_Costello.pdf.
30. James McBride, Andrew Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?" Council on Foreign Relations. http://web.archive.org/web/20181106080952/https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.
31. Ellen Nakashima, "Chinese breach data of 4 million federal workers," Washington Post, June 4, 2015.
32. NBC News, "Clapper Calls China 'Leading Suspect' in OPM Hack," www.nbcnews.com. https://www.nbcnews.com/video/clapper-calls-china-leading-suspect-in-opm-hack-471284803815.
33. Jack Moore, "Intelligence Chief: OPM Hack Was Not a 'Cyberattack'." Nextgov. http://web.archive.org/web/20210507121532/https://www.nextgov.com/cybersecurity/2015/09/intelligence-chief-clapper-opm-hack-was-not-cyberattack/120722/.
34. David Sanger, "U.S. Decides to Retaliate Against China's Hacking." New York Times. 31 07. http://web.archive.org/web/20150803091159/https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html.
35. Zach Dorfman, "China used stolen data to expose CIA operatives in Africa and Europe." Foreign Policy Magazine. 21 12. https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/.
36. Department of Justice, "Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax." justice.gov. http://web.archive.org/web/20200210152747/https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.
37. Department of Justice, "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information." doj.gov. http://web.archive.org/web/20181221022038/https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.
38. Department of Justice, "Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally." doj.gov. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.
39. Department of Justice, "Attorney General Jeff Sessions Announces New Initiative to Combat Chinese Economic Espionage." justice.gov. https://www.justice.gov/opa/speech/attorney-general-jeff-sessions-announces-new-initiative-combat-chinese-economic-espionage.
40. Christopher Bing, "White House blames Russian spy agency SVR for SolarWinds hack: statement." Reuters. http://web.archive.org/web/20210416060945/https://www.reuters.com/business/white-house-blames-russian-spy-agency-svr-solarwinds-hack-statement-2021-04-15/.
41. Foreign, Commonwealth & Development Office, "Russia: UK and US expose global campaign of malign activity by Russian intelligence services." gov.uk. http://web.archive.org/web/20210420062545/https://www.gov.uk/government/news/russia-uk-and-us-expose-global-campaigns-of-malign-activity-by-russian-intelligence-services.
42. Dustin Volz, "In Punishing Russia for SolarWinds, Biden Upends U.S. Convention on Cyber Espionage," *Wall Street Journal,* http://web.archive.org/web/20210417093441/https://www.wsj.com/articles/in-punishing-russia-for-solarwinds-biden-upends-u-s-convention-on-cyber-espionage-11618651800.
43. Paul Kolbe, "With Hacking, the United States Needs to Stop Playing the Victim," *New York Times,* https://www.nytimes.com/2020/12/23/opinion/russia-united-states-hack.html.
44. Andy Greenberg, "US Sanctions on Russia Rewrite Cyberespionage's Rules." Wired Magazine. http://web.archive.org/web/20210415195202/https://www.wired.com/story/us-russia-sanctions-solarwinds-svr/.
45. Perri Adams, Dave Aitel, George Perkovich, JD Work, "Responsible Cyber Offense," *Lawfare Blog,* http://web.archive.org/web/20210805122236/https://www.lawfareblog.com/responsible-cyber-offense.

❖ ❖ ❖