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

Lester Godefrey

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

The views, opinions, and findings of the author expressed in this article should not be construed as asserting or implying US government endorsement of its factual statements and interpretations or representing the official positions of any component of the United States government.
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.

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.”

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-counter-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.”

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.

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). 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. 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.

Espionage Norms

Espionage is largely uncodified in international law. Instead, it is governed by explicit and implicit norms within the international system. 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. 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.
An Allied Perspective on Cyber

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 interception 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 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 Operations16 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.

---

1. 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.
Studies in Intelligence Vol. 66, No. 1 (Extracts, March 2022)

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. 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.

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). 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.

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, heightened 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.

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.

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

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?” Former CIA intelligence officer Paul Kolbe concurred, arguing that the US is “engaged in the same type of operations at an even grander scale.”

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.

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 countermessages 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 countermessages 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 categorizations of unacceptable behaviors in cyber operations and communicating them to adversaries can create opportunities for threat actors to operate just under escalation thresholds. Ferri 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 Godfrey is the pen name of a UK government analyst.
Endnotes

2. William Johnson, Thwarting Enemies at Home and Abroad (Georgetown University Press, 1987).


