Spying and Fighting in Cyberspace: What is Which?

Gary Brown*

Introduction

Traditionally, espionage has inhabited a niche between order and chaos. States have recognized the existence of espionage and enacted domestic legislation to prohibit it, but international law is silent on the subject.[1] On the other hand, States accept espionage as part of the business of international relations and are generally tolerant of it. That may be changing, however. Cyberspace, especially the Internet, has become an integral part of everyday life. The use of cyberspace for espionage has generated difficult discussions about the nature of cyberspace, the extent of national sovereignty, and the importance of individual privacy, among other issues, all of which are relevant in a conversation about espionage. This article focuses on another issue, which is the overlap of espionage and aggressive cyber operations. Confusion about the intent behind an intrusion could lead to a misreading of aggressive intent, unnecessary escalation of tensions, or a false sense of security in the opening act of significant cyber aggression. This article also discusses the United States' stance on dividing espionage into categories depending on the purpose.

Rapid improvements in computer technology and techniques, as well as the exponential rise in the amount of data stored online, have driven a closer look at the subject of cyber espionage, in particular how it differs from traditional methods of spying. The speed of access and exfiltration in cyber espionage operations can rapidly result in libraries of information, dwarfing the information that can be obtained through more traditional methods of espionage.[2] Although some of the issues discussed here are also relevant in traditional espionage operations, they have seemed less so in the past. They may have

* Gary Brown is a professor of Cyber Security at Marine Corps University.

1. It could be cited as an exception that the International Court of Justice directed Australia to refrain from interfering with communications between Timor-Leste and legal advisers regarding current and future legal actions. *See* Press Release, Int'l Court of Justice, Questions relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), Int'l Court of Justice (Mar. 3, 2014), http://www.icj-cij.org/docket/files/156/18076.pdf. That case stands as a solitary assertion, however, and applies to the special relationship between counsel and client, making its value as precedent questionable.

2. Verizon's 2015 *Data Breach Investigations Report* notes that in 60% of cases, cyber operators are able to compromise a target organization within minutes. Verizon, 2015 Data Breach Investigations Report 6, http://www.verizonenterprise.com/DBIR/2015. The 2014 Sony hack resulted in around 100 terabytes of data being stolen, an amount of data that, if stored on CD-ROMs, would require a stack of them 3,900 feet high. *See* Kim Zetter, *Sony Got Hacked Hard: What We Know and Don't Know So Far*, Wired (Dec. 3, 2014), http://www.wired.com/2014/12/sony-hack-what-we-know; Joel Lee, *Memory Sizes Explained – Gigabytes, Terabytes & Petabytes in Layman's Terms* (Aug. 14, 2012), http://www.makeuseof.com/tag/memory-sizes-gigabytes-terabytes-petabytes.

come to the forefront now because of the effectiveness and pervasiveness of cyber espionage. This article will focus only on cyber methods of espionage.

The United States defines espionage as "[t]he act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation."[3]

The distinction between cyber espionage and more aggressive cyber operations is critical under international law. Espionage has been considered unregulated under the international legal system – meaning cyber activities that constitute espionage are neither lawful nor unlawful under international law.[4] As a result, States freely engage in espionage and generally accept it from other States, with results limited to punishing spies under domestic law and the expulsion of diplomats. This is in stark contrast to the treatment of aggressive activity, which might constitute an illegal use of force under the U.N. Charter.[5]

I. NOT ALL ESPIONAGE IS EQUAL

Historically, the United States appears to have agreed that international law should not apply to traditional espionage and that instead the punishment of spies should be left to domestic law. With the rise of cyber espionage, however, the United States has begun to change its position.[6] "Traditional espionage encompasses a government's efforts to acquire clandestinely classified or otherwise protected information from a foreign government," explains cyber security expert, David P. Fidler. "Economic espionage involves a State's attempts to acquire covertly trade secrets held by foreign private enterprises."[7] The United States manifested this distinction in the unprecedented indictment of five Chinese military officers for engaging in cyber espionage from China, in Administration statements critical of economic espionage, and in the U.S.-China agreement prohibiting cyber economic espionage for commercial gain, but is silent on other categories of espionage.[8]

---

3. U.S. DEP'T OF DEFENSE, JOINT PUBL'N 1-02: DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 82 (2015). *Accord* 18 U.S.C. § 794 (2012).

4. Whether or not espionage is prohibited by international law does not affect whether it may be prohibited or otherwise regulated domestically.

5. U.N. Charter art. 2, ¶ 4.

6. S*ee* John Carlin, Assistant Attorney Gen. for Nat'l Sec., Dep't of Justice, Assistant Attorney General John Carlin Delivers Remarks at the Brookings Institute's Emerging National Security Threats Forum (May 22, 2014), http://www.justice.gov/nsd/pr/assistant-attorney-general-john-carlin-delivers-remarks-brookings-institutes-emerging; Greg Austin, *China's Cyberespionage: The National Security Distinction and U.S. Diplomacy,* THE DIPLOMAT (May 2015), http://thediplomat.com/wp-content/uploads/2015/05/thediplomat_2015-05-21_22-14-05.pdf (discussing U.S. position).

7. David P. Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies*, 17 ASIL INSIGHTS NO. 10 (Mar. 20, 2013).

8. *See U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage* (U.S. Dep't of Justice, Washington, D.C.), May 19, 2014, http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-

In February 2013, the cyber security company Mandiant published a compelling portfolio of evidence tying the Chinese military to cyber economic espionage. That Mandiant chose commercial espionage for its deep-dive investigation appears to reflect the U.S. position that "economic espionage" should be treated differently than more traditional or "national security espionage."[9]

The United States treats as traditional espionage the theft of information more directly relevant to national security. U.S. concern over cyber espionage was reflected by then-National Security Agency Director, General Keith Alexander when he said "the loss of industrial information and intellectual property through cyber espionage constitutes the 'greatest transfer of wealth in history.'"[10] Although General Alexander's statement has been criticized as exaggerated, there does appear to be a large, on-going transfer of possession of intellectual property through cyber-enabled espionage.[11]

If espionage is to be split into two distinct categories, it may seem counterintuitive that economic espionage would be the more disfavored category. After all, economic espionage merely transfers net wealth and marginally decreases the incentive to innovate.[12] It might make sense to treat economic espionage less seriously than traditional espionage, as the latter could directly and negatively affect national security. The United States has decided the opposite is true, perhaps because espionage directly benefiting national security is considered to have a longer, more established tradition. In addition, national security espionage may have come to be tolerated among States because it distributes knowledge that may increase the collective security of the community of nations by reducing surprise, increasing knowledge of intentions, etc.

---

against-us-corporations-and-labor. [hereinafter *U.S. Charges*]; *National Security Advisor Susan E. Rice's As Prepared Remarks on the U.S.-China Relationship at George Washington University* (The White House, Washington, D.C.), Sept. 21, 2015, https://www.whitehouse.gov/the-press-office/2015/09/21/national-security-advisor-susan-e-rices-prepared-remarks-us-china; *Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference* (The White House, Washington, D.C.), Sept. 25, 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

9. MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

10. Josh Rogin, *NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History,"* FOREIGN POL'Y (July 9, 2012), http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history.

11. The U.S. Department of Commerce estimates intellectual property theft from U.S. companies amounts to $200 to $250 billion annually. *Stolen Intellectual Property Harms American Businesses Says Acting Deputy Secretary Blank* (U.S. Dep't of Commerce), Nov. 29, 2011, http://www.commerce.gov/blog/2011/11/29/stolen-intellectual-property-harms-american-businessessays-acting-deputy-secretary-. The Commission on the Theft of American Intellectual Property estimated the annual loss to be $300 billion. COMM'N ON THE THEFT OF AM. INTELLECTUAL PROP., THE IP COMMISSION REPORT 2 (May 2013), http://www.ipcommission.org/report/ip_commission_report_052213.pdf.

12. Christina Parajon Skinner, *An International Law Response to Economic Cyber Espionage*, 46 CONN. L. REV. 1165, 1183-4 (2014).

In any event, there has been no clear international consensus that singles out economic espionage for denunciation.[13] Currently, State responses to economic espionage include official condemnation, responsive sanctions or the use of other international tools to dissuade economic espionage. None of these indicate that it is treated differently than national security espionage.

Even if there were a concerted international movement to recognize the distinction between "good" and "bad" espionage, the details, at least to some degree, would be challenging. National security is a broad concept. It includes not just military forces, but also political stability – and the strength of the economy.[14] Rational arguments can be made for a vast array of technologies contributing to "national security." For example, energy technologies can benefit the military, food technology can increase a State's self-sufficiency, and entertainment technology can increase the effectiveness of propaganda. The *Commentary to Additional Protocol I* notes that all information has some relevance for national security, and this is especially relevant with regard to cyber espionage.[15]

II. ARE WE UNDER ATTACK?

Although the United States is engaged on the issue of categories of espionage, it has said little about the challenge of distinguishing between identical cyber activities undertaken for fundamentally different purposes. For instance, will virtual presence on a cyber system, without more information, be treated as espionage, remaining essentially unregulated, or be treated as preparation for cyber warfare akin to penetrating sovereign airspace with armed fighters or massing armed forces on the border?

In the purely physical world it is usually simple to distinguish espionage from bellicose activity. The weapons used to fight a war are generally distinguishable from those used to spy, both in nature and in quantity. For example, if a spy is armed at all it is likely with a sidearm or other light weapon. Spies usually work alone or in small groups. Basically, traditional spies look like ordinary citizens, or at most like ordinary criminals. It is often the intent of spies to look like insiders, or people who have permission to be where they are. Troops planning to engage in combat, on the other hand, appear to be what they

13. It is too early to tell whether the U.S.-China agreement signals a change in the general international approach to the issue.

14. It is frequently noted that China sees its economy and national security as two sides of the same coin. *See* Rana Foroohar, *What Chinese Cyber-Espionage Says about the Chinese (and U.S.) Economy*, TIME (May 20, 2014, http://time.com/105910/chinese-spying-economy-hacking-espionage. The United States' 2010 National Security Strategy mentions aspects of the economy 50 times; it is clearly important to the U.S. vision of national security, as well. *See* 2010 WHITE HOUSE, NAT'L SEC. STRATEGY, https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

15. *See* CLAUDE PILLOT ET AL., INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 566 (Yves Sandoz et al. eds., 1987).

are – combatants.[16] Combatants are required to wear uniforms and carry their arms openly. They are normally armed with heavier weapons and present in larger numbers. These facts, together with the location of the individuals involved, generally make a determination of whether a particular activity is espionage relatively straightforward in the physical world.

Some cyber attacks are easy to define. For example, gaining access to a computer network and using the access to physically destroy attached computers or equipment is a cyber attack. In more subtle cases, however, it can be difficult for the party on the receiving end of a cyber operation to distinguish between espionage and military attack (including actions leading up to an attack). Most cyber operations of any type require gaining unauthorized or secret access to an information system.[17] When victims discover their cyber systems have been penetrated, determining what happened and whether information has been stolen or modified may not be easy if the attacker is patient and careful. It is often not immediately apparent whether the unauthorized access is intended for spying, for disruptive and destructive activities, or both. The potential damage is not limited to a physical location, as in the case of a saboteur, which ups the ante for cyber operations. To complicate the situation even more, the initial access may be for reconnaissance in advance of attack, so that the compromise and theft of data are preludes to future offensive operations. Finally, even if the initial purpose were espionage, access itself may embolden the hacker to commit a future attack.

Both espionage and warfighting benefit from acquiring access to as many systems as possible, to maximize either information gathering or the effect of a future attack. Given the nature of cyberspace, that might mean thousands of systems for either type of operation. Accordingly, both quantitatively and qualitatively, espionage and warfighting in cyberspace can be indistinguishable until the denouement.

Although merely gaining access to a network or computer is not a wrongful use of force or an armed attack under international law, the *method* used might be.[18] Some cases are simple. Invading a military base located across a national border, causing hundreds of casualties, for the purpose of seizing a hard drive containing sensitive information is not espionage – even if that is the sole purpose of the excursion. It is a military attack. More subtle examples can be difficult to parse. To facilitate espionage, a State might covertly dispatch a small military unit to break into a secure facility for the purpose of inserting a flash drive into a network to upload malware that will enable the collection of

16. Camouflage is a kind of "deception" perhaps, but the deconstruction of "cyber camouflage" I'll leave to someone else.

17. Herbert Lin discusses these different actions in *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SECURITY L. & POL'Y 63, 64 (2010).

18. *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 195 (Michael N. Schmitt ed., 2013). The concepts of use of force and armed attack are from the U.N. Charter art. 2 ¶ 4, 51.

information. The smaller the unit, and the less force used, the greater the likelihood the action will be seen as espionage – but at some point, such endeavors constitute a significant breach of sovereignty or a wrongful use of force in violation of international law.

Similarly, cyber activities undertaken for the purpose of collecting intelligence might look like cyber attacks. The U.S. National Research Council has observed that there may be situations where "the distinction between a cyberattack and [cyber intelligence gathering] may be very hard to draw from a technical standpoint, since both start with taking advantage of a vulnerability."[19] Both offensive cyber activity and cyber espionage rely on acquiring unauthorized access to a system, and that often involves damaging a system in some way. The damage may be reducing the effectiveness of the target system's anti-virus software, decreasing the effectiveness of its encryption programs, installing a back door or altering its operating system, for example. If damage is defined to include activities that decrease effectiveness or cause a system to cease its intended function, then each of these is an illustration of damaging the targeted system.[20]

The overlap of espionage and offensive operations in cyberspace appears to have been recognized and has been addressed through policy and doctrinal definitions in the United States. Cyber espionage is referred to as "computer network exploitation," which is defined as "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[21] The critical phrase is "enabling operations," which includes cyber activity that would otherwise be considered a cyber attack as noted above. That is, an enabling operation could logically include physically damaging one system to facilitate the gathering of intelligence from another system.

"Enabling" is distinct from the collection of intelligence; it is rather those things that permit the collection. As discussed above, these could include anything from a physical presence in a foreign computer center to damaging systems to make them exploitable. Of course, it also includes collateral actions necessary to collect intelligence, such as forcing a computer reboot to install malware or sending a phishing email, which are not, standing alone, the collection of intelligence. Some of these collateral activities are cyber attacks, but they are defined as part of an intelligence operation. This is a definitional overlap between two fundamentally different categories of activity.

Occupying the space between cyber espionage and cyber aggression is Operational Preparation of the Environment (OPE). The Department of Defense

19. TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 261 (William A. Owens et al. eds., 2009).

20. This concept of damage is also discussed below. *See* discussion *infra* Section III.D.

21. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-695R, DEF. DEP'T CYBER EFFORTS: DEFINITIONS, FOCAL POINT, AND METHODOLOGY NEEDED FOR DOD TO DEVELOP FULL-SPECTRUM CYBERSPACE BUDGET ESTIMATES 2 (2011).

defines OPE as "[t]he conduct of activities in likely or potential areas of operations to prepare and shape the operational environment."[22] OPE could include cyber operations to penetrate systems, introduce malware or undertake other actions in preparation for offensive action. These activities occur in the absence of armed conflict, although conflict may be anticipated.

Pre-positioning cyber capabilities on networks or computer systems, by itself, does not constitute cyber aggression, and is not quite espionage, because it is not collecting intelligence. This activity is rather some unique category falling between espionage and attack. Although capabilities are prepositioned in the kinetic world as well, the legal issues are easier to deal with in the physical world. For example, there is little doubt that concealing a weapons cache in another State's territory is preparation for armed attack. On the other hand, obtaining access to a system often fails to signal what kind of follow-on action is anticipated. This ambiguity is one thing that makes cyber operations uniquely challenging.

Similarly, many pre-positioned capabilities provide the ability to engage in either espionage or aggressive activity, and so acting to emplace these capabilities may be mistaken for either of the other two. For example, malware that allows its controller to log on a system with administrator privileges would provide the opportunity to view or copy information on a network, as well as delete information and take other actions that could physically damage the system, i.e., constitute an attack. Obtaining and maintaining this kind of pre-positioned capability could be seen as the equivalent of planting explosives to be used at a future point.

This article will not address cyber OPE as a unique category. Although there are doctrinal and policy reasons for treating it as distinct, OPE can be included in this discussion by looking at it as an intelligence activity that has the potential to be mistaken for aggression.

III. A FRAMEWORK FOR ANALYSIS

There are more commonalities than distinctions between cyber espionage and cyber aggression. The framework below provides a broad overview of the steps involved in cyber operations, followed by brief vignettes drawn from actual events that apply the framework. This analysis helps delineate the gray areas between cyber espionage and other cyber operations.

Put simply, any cyber operation requires identification, penetration, presence, exploitation and harm. I illustrate this using a pretend state-sponsored hacker named P0wn$z.

The first requirement for any operation is determining the target. The **identification** of a cyber system is the least elegant step. P0wn$z might do this by using a bot to conduct a massive survey of cyber systems, seeking out those

22. U.S. DEP'T OF DEF., JP 1-02, DEP'T OF DEF. DICTIONARY OF MIL. AND ASSOCIATED TERMS (2015).

with typical characteristics for the system he wants to target; for example, some SCADA systems have characteristics that make them easy to spot on the Internet.[23] P0wn$z will be looking for the type of systems he wants that have vulnerabilities, such as unpatched software or unchanged default passwords. In this way, P0wn$z can build an extensive database of potential targets that he can sell to the highest bidder or use for his own purposes.[24]

Once P0wn$z finds the system he wants to target, initial **penetration** of a system can be accomplished in a variety of ways. For Stuxnet, the cyber operation that destroyed nuclear centrifuges in Iran, it was through a worm.[25] In the case of Operation Buckshot Yankee,[26] it was most likely effected by the strategic placement of flash drives containing malware that were eventually used on official systems. Many system penetrations use the tried and true method of phishing emails, which are often cleverly crafted using information available from social media. Regardless of the method, the purpose is to gain and elevate access to the target system. That is, the goal is to get on the system and ideally to gain credentials as a system administrator.

After gaining access, the next thing P0wn$z wants to do is establish a persistent **presence** on the system. Operating systems and anti-virus software may be updated and passwords may change, for example. P0wn$z wants to access the system repeatedly. To exfiltrate large amounts of data, P0wn$z will spread the downloads over the course of several days or weeks to avoid being noticed by network monitoring tools. Besides, new information will be added to the system constantly, and a persistent access may yield results for many years. To establish persistent access, P0wn$z may install additional malware or create additional accounts on the system, for example, to provide a back door for future use.

The fourth step in the operation is **exploitation** of the access to gain information. As noted above, this may involve the exfiltration of information to a server located anywhere in the world, from where P0wn$z can move it later to where it will be analyzed. Exploitation might also involve real time monitoring of email content or system usage data to get inside the decision loop of the target organization. Another use of exploitation is to gather system information so that the system itself can be degraded or damaged.

Using the information to cause **harm** is the ultimate goal of a cyber operation, whether espionage or military. An espionage operation would seek to use the information gathered to do damage to the national security of the target

23. ICS-CERT noted the ease of identifying some of these systems in Dep't of Homeland Sec., *Incident Response Activity*, ICS-CERT MONITOR, Jan.-Apr. 2014, at 1, 2.

24. Some of the methods used to identify vulnerable systems are set out in Pedram Hayati, Presentation at the 2015 Hack In The Box Security Conference: Uncovering Secret Connections Among Attackers by Using Network Theory and Custom Honeypots (May 28, 2015).

25. *See* Kim Zetter, COUNTERDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON (2014).

26. *See* III.B. below.

State. In some cases, the target's national security is weakened because a potential adversary has learned some strategic secret, such as where troops plan to strike, or a technical secret such as how to defeat a radar system. In some cases, the relative security of the victim State is reduced because a rival State has narrowed the victim's lead in some strategic technology. In either case, the spying State benefits and the target State suffers a detriment. It could be argued that no harm is intended or follows when "friends" spy on "friends," as when the United States obtained access to the German Chancellor's cellphone.[27] The term "harm" as defined here includes changes in the relative advantage between States, because spying friends are potential future adversaries. As Henry Kissinger famously noted, "America has no permanent friends or enemies, only interests."[28]

As noted earlier, the United States sees a subset here. According to the United States' view, using the pilfered information for commercial gain is fundamentally different from using it for the advancement of national security.[29] China, however, has asserted that a State's economy is an essential part of its national security, so damaging one State's economy or benefiting the economy of another is the same as any other use of information obtained through espionage.[30] Whether one position is preferable in law will not be discussed here. It can also be difficult to determine whether a particular operation is undertaken for the purpose of commercial gain or whether it incidentally results in commercial gain. This difficulty in distinguishing between the facts underlying the two positions is addressed in the scenarios below.

In more aggressive operations the harm intended might be actual damage to the host computer system, destruction of critical data, or damage to industrial systems connected to the network, for example. The important thing to note is that penetration, presence and exploitation may be precisely the same, whether the operation is intended for espionage or aggression. It is only with the harm that the two types of operation become distinguishable. This similarity throughout most of the operation creates challenges for legal and policy frameworks, as will be evident in the description of the operations below.

The examples below illustrate how penetration, presence, exploitation and harm apply in some publicly reported cyber operations. The crucial first step of

---

27. *Embassy Espionage: The NSA's Secret Spy Hub in Berlin*, DER SPIEGEL (Oct. 27, 2013), http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.

28. Kissinger was echoing a classic foreign policy position. This international reality is what made the 2010 revelation of the no spying agreement among the "Five Eyes" countries so surprising. Gordon Corera, *Spying Scandal: Will the 'Five Eyes' Club Open up?*, BBC (Oct. 29, 2013), http://www.bbc.com/news/world-europe-24715168.

29. Shannon Tiezzi, *China's Response to the U.S. Cyber Espionage Charges*, THE DIPLOMAT (May 21, 2014), http://thediplomat.com/2014/05/chinas-response-to-the-us-cyber-espionage-charges.

30. In the end, there may be little difference between the United States a and Chinese views on this matter, though the United States tends to phrase its position in terms of how the loss of information harms its national security rather than how obtaining it would improve its security. *See* EXEC. OFFICE OF THE PRESIDENT, ADMIN. STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS 3 (2013).

identification is left for another paper, as it is focused on technology and intelligence collection rather than policy and law.

A. Undersea Cable Tapping

Cable tapping is discussed as a cyber operation because most Internet traffic passes through submarine cables. The United States has reportedly collected information from undersea communications cables for years. In the 1970's the United States attached recording boxes to Soviet undersea cables.[31] Later, the United States (and others) may have tapped into submarine cables at repeater junctions under the sea.[32] From published reports, this appears to be a blended cyber-kinetic method that introduces a new item of physical equipment to a system to collect cyber intelligence. An operation that collects such huge amounts of information is a gold mine of espionage. The *penetration* of the undersea cables that cumulatively carry 99% of the world's Internet traffic was most likely accomplished through a variety of physical means.[33] As espionage equipment was physically attached to the cables, it continued to maintain the *presence* on the system. The exploitation was through a variety of means, as well, the most entertaining being the divers retrieving tapes from Soviet cables every few weeks.[34]

The complicating factor in this operation is the scale. If all the data moving through the cable is collected, it includes both national security and purely commercial data – and, of course, an enormous amount of personal information that raises constitutional issues beyond the scope of this article. The physical devices designed to be attached to undersea cables could include the capability to jam or otherwise interfere with electronic traffic passing through the cables. This would be an especially desirable way to deny communications during a conflict, because the system could be restored essentially cost-free after the conflict. Even in a case like this one that seems like simple espionage, the technology injects an element of doubt concerning the actor's intentions. The mere *presence* on the system could be espionage or preparing for conflict.

B. Operation Buckshot Yankee (OBY)

In 2008, DoD's classified military computer networks were compromised by malware. A flash drive pre-loaded with targeted malware was inserted into a military laptop at a base in the Middle East. The malicious code copied itself onto U.S. Central Command's computer network, from where it spread across the military system, infecting both classified and unclassified computers. The

31. Olga Khazan, *The Creepy, Long-Standing Practice of Undersea Cable Tapping*, THE ATLANTIC (Jul. 16, 2013), http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855.

32. *Id.*

33. *What the Internet looks like: Undersea Cables Wiring ends of the Earth*, CNN, Jan. 2, 2015, http://www.cnn.com/2014/03/04/tech/gallery/internet-undersea-cables.

34. Khazan, *supra* note 31.

purpose of the malware was to discover what information was available on the network, report back to its controller and then exfiltrate desired information. DoD concluded the malware was distributed by a foreign intelligence agency.[35]

Perhaps the most interesting feature of the malware used here was its ability to jump the air gap between the classified and unclassified computer systems, a capability critical to the success of the Stuxnet operation.[36] When legitimate users used a flash drive to transfer information between systems, the malware was designed to ride the flash drive for the initial infection, and later to cause information to hitchhike on the drive from the classified to the unclassified system. From the unclassified system, sensitive information could be transferred over the Internet.[37]

OBY was a straightforward cyber espionage operation. It appeared to target an official information system with the intent of gathering national security information to use for national security purposes. There were no reports that the malware used was capable of damaging the compromised system, so there was little chance of mistaking the intent of the spying State.

C. F-35 Plans

Although few details have been released, in 2007 China hacked U.S. government contractor computer networks and obtained millions of pages of F-35 (also referred to as the Joint Strike Fighter or JSF) technical data.[38] "According to a report from *Independent Journalism Review*, the U.S. Naval Institute speculates that the J-31 was 'designed using technology stolen from the Pentagon's nearly $400 billion Lockheed Martin F-35 Joint Strike Fighter program.'"[39]

This may at first appear to be another typical espionage case, and perhaps it is. It also helps illuminate the complexity of applying the U.S. position on good and bad espionage. U.S. officials noted that the theft of this data caused great damage to U.S. interests, giving away a substantial U.S. advantage in aviation, while reducing the lead time and costs to adversaries working to develop stealth

35. William J. Lynn III, *Defending a New Domain,* FOREIGN AFFAIRS (Sept./Oct. 2010), https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

36. "An air-gapped computer is one that is neither connected to the internet nor connected to other systems that are connected to the internet." Kim Zetter, *Hacker Lexicon: What Is an Air Gap?*, Wired (Dec. 8, 2014), http://www.wired.com/2014/12/hacker-lexicon-air-gap/.

37. *U.S. Cyber Command: Organizing for Cyberspace Operations: Before the H.Comm. on Armed Services*, 111th Cong. 10 (2010) (statement of General Keith Alexander, Commander, U.S. Cyber Command), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg62397/pdf/CHRG-111hhrg62397.pdf.

38. Ellen Nakashima, *Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies*, WASH. POST (May 27, 2013), https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

39. *U.S. Pilots Say New Chinese Stealth Fighter Could Become Equal of F-22, F-35*, USNI NEWS, (U.S. Naval Inst., Annapolis, Md.), Nov. 5, 2014, http://news.usni.org/2014/11/05/u-s-pilots-say-new-chinese-stealth-fighter-become-equal-f-22-f-35.

technology themselves.[40] The harm that resulted to the United States' lead in stealth aircraft technology and the benefit to China's program are typical of espionage operations. The pertinent distinction here is that the information was apparently given to a manufacturer, Shenyang Aircraft Corporation, which presumably profited from it, while improving China's air force and national security.[41] Where is the line between strategic technology and private sector technological advances? It may be difficult to draw. For example, solar power could make troop deployments more efficient by reducing fuel needs. Automobile technology may improve military vehicles. An advance in health sciences may improve battlefield medicine. Virtually any manufacturing technology can be related to national security.

D. Equation Group

This recently reported case is an example of supply chain exploitation. It simplifies the job of spying if the target's hardware is manipulated in advance to permit unauthorized access. In this case, a State's security service is reported to have installed capabilities on firmware (basically built-in software that controls the hardware) before it arrived at its destination. As reported, "[t]he malicious firmware created a secret storage vault that survived military-grade disk wiping and reformatting, making sensitive data stolen from victims available even after reformatting the drive and reinstalling the operating system."[42]

In this case, *penetration* and *presence* occur before the equipment becomes the target; *exploitation* is available as soon as it is worthwhile. Although this capability may not be able to damage the system directly, if you cannot use the targeted device as intended any more, but it still works, has there been an attack? If a system contains any sensitive information, once the penetration is discovered, the hardware is not usable. Functionally, it has been destroyed. Because of the time involved in an operation of this type, there is less risk of escalation, but there is still the question of characterization. Is it merely espionage when the process requires functionally destroying the target system? Once again, the scale of all things cyber may play a role. Destroying a few items in the name of espionage may mean little. What if a supply system penetration is discovered that affected hundreds of thousands of computer chips, routers or other components? At some point, it seems this could become something more than simply spying.[43]

---

40. *China's Cyber-Theft Jet Fighter*, WALL ST. J., (Nov. 12, 2014), http://www.wsj.com/articles/chinas-cyber-theft-jet-fighter-1415838777?alg=y.

41. Jack Mulcaire, *China's Stealth Fighters: Ready to Soar?*, THE NATIONAL INTEREST: THE BUZZ (April 16, 2014), http://nationalinterest.org/blog/the-buzz/chinas-stealth-fighters-ready-soar-10252.

42. Dan Goodin, *How "Omnipotent" Hackers Tied to NSA Hid for 14 Years – and Were Found At Last*, ARS TECHNICA, (Feb. 16, 2015), http://arstechnica.com/security/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/.

43. *See id.*

E. SCADA Systems

Utilities and modern manufacturing processes are often managed by computerized industrial control systems, most commonly referred to as Supervisory Control and Data Acquisition (SCADA) systems.[44] SCADA systems are vital in the modern industrial world, controlling things as critical as drinking water plants, steel processing, auto manufacturing and electrical power grids. SCADA systems are designed for long lifespans and reliability, with security often considered a lower priority. They do not contain much information of interest, except to those who might be planning a cyber attack on the system. On the other hand, the lack of security on a networked SCADA system can make it an inviting target for hackers hoping to gain access to connected systems. For example, the massive breach of Target's computer system appears to have been facilitated by computer credentials stolen from the company's air conditioning service provider.[45] That incident resulted in the exposure of 70 million Target customers' personal data.[46] Thieves and military planners may have good reasons for hacking into SCADA systems – but spies remain problematic.

Because States do not store secrets on utility systems, and the systems generally contain only information about the utilities themselves, any information that could be obtained from a SCADA system is probably only useful as reconnaissance for a future attack.[47] Does it follow that merely establishing persistent *presence* on a SCADA system could be taken as aggressive? In most cases the intelligence value of any information is so low that analysts might assume the operation is not an exercise in simple espionage, but rather a prelude to aggression. U.S. SCADA systems are frequently targets of cyber operations.[48] The potential *harm* is considerable. Espionage and operations with more aggressive intent seem particularly difficult to distinguish in these cases. In 2014, a hacker caused "massive damage" to a steel plant in Germany.[49] Just before the final step, it may have been impossible for an administrator of the steel plant's systems, having discovered a hacker inside the system, to know whether the intruder was in the final stages of preparing for the destructive attack or merely spying, which creates a risk of miscalculation.

---

44. SCADA is the term most generally recognized in legal and policy discussions about cyber operations to describe computer systems that facilitate the remote control of industrial and utility systems, even when the systems might more accurately be described as Industrial Control Systems or IP Addressable Appliances. The last term best describes the system at Target.

45. Mathew J. Schwartz, *Target Breach: HVAC Contractor Systems Investigated*, DARK READING (Feb. 6, 2014), http://www.darkreading.com/attacks-and-breaches/target-breach-hvac-contractor-systems-investigated/d/d-id/1113728.

46. *Id.*

47. John Hultquist, *Sandworm Team – Targeting SCADA Systems*, iSIGHT PARTNERS: BLOG (Oct. 21, 2014), http://www.isightpartners.com/2014/10/sandworm-team-targeting-scada-systems/.

48. Joel Langill et al., *Cyberespionage Campaign Hits Energy Companies* (July 8, 2014) (on file with Security Matters), http://www.secmatters.com/sites/www.secmatters.com/files/documents/whitepaper_havex_US.pdf.

49. Kim Zetter, *A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever*, WIRED (Jan. 8, 2015), http://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

A final case that may help bring all the threads together is the 2014 Sony hack.[50] In that incident, hackers gained access to Sony's computer network. The hackers released a huge amount of business data, emails, personal data of employees, salary information, full copies of unreleased movies, and more. At some point the operation took a hostile turn and destroyed data on the servers.

The facts of the incident work well for this discussion if we speculate about a similar attack on FBI servers. In such a case, the FBI might detect the intruders at an early phase of the operation: while they are penetrating the federal computer system, establishing a persistent presence or exfiltrating sensitive anti-terrorism data, for example. At any of these times, it would appear to be nothing more than an espionage case. Then, perhaps without warning, the operation might turn aggressive. The same malware capabilities used to exfiltrate data might be used to delete (i.e., destroy) data and to render much more data inaccessible by corrupting the master boot records of hard drives.[51] Would such a virtual destruction of a critical government information system rise to a level justifying a kinetic response? The United States acknowledged the possibility that a cyber operation could justify actions in self-defense in its 2011 *International Strategy for Cyberspace*: "When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country."[52] If an apparent espionage operation can so quickly turn destructive, at what point is a State justified in aggressively acting in anticipation of a cyber attack?[53]

CONCLUSION

As discussed here, the tactics and techniques used in espionage and military operations in cyberspace are often identical. Although when reviewing the results of cyber activity, it may be easy to determine what the purpose of the action was, mid-operation – when responses are being considered – there is great potential for international misunderstanding and miscalculation. There is not an easy fix; it is simply a situation with which the international community must contend. Espionage will continue to be required as part of a responsible strategy prior to military action, and there is no indication the world's "second

50. Information on the Sony incident is drawn from Zetter, *supra* note 2, and Michael Mimoso, *Details Emerge on Sony Wiper Malware Destover*, Threat Post (Dec. 4, 2014), https://threatpost.com/details-emerge-on-sony-wiper-malware-destover/109727/.

51. Deleting the master boot record of a hard drive makes it practically impossible to access the data on the drive, even though it is still present.

52. *See* EXEC. OFFICE OF THE PRESIDENT, INT'L STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 14 (2011), https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

53. Of course, the difficulty of attributing cyber actions to a particular State could mean that the target of aggressive self-defense would be uncertain, but that just makes the situation more dangerous, as even uncertain national leaders might feel compelled to "do something" to demonstrate to a restive population they are still in control.

oldest profession" will end even in the absence of aggressive intent, because it supports economic and diplomatic strategies, as well.

The observation that for a significant duration of a continuous cyber event it is impossible to distinguish between espionage, preparing the environment for a cyber attack, and the beginning of a cyber attack is unlikely to change the behavior of States. Despite the potential pitfalls set out here, States will continue to pursue courses of action – in this case the cyber options – they think best serve their own interests. Cyber espionage in particular is likely to continue to increase, as it results in the collection of huge amounts of strategic data for intelligence agencies. Rather than focusing on the unattainable, policy efforts would be better spent elsewhere. States should not attempt to create a different standard for cyberspace espionage, and for different types of espionage in cyberspace. Often, military operations in cyberspace and cyber espionage are distinguishable only by intent, which is difficult or impossible for the victim to ascertain. States should rather focus on the actual actions, as it is the behavior and the effects that determine international legality, not the intent of the actor. States might be reluctant to agree to stop engaging in strategically lucrative activity in return for increased international cooperation, but the expedient path of trying to divide cyber activities into categories of good and bad does not seem to have resulted in increased international understanding about state-sponsored cyber activities.

In a loosely governed environment like cyberspace, a shared understanding of the boundaries on acceptable behavior may be the best way to avoid unnecessary tension, or even escalation to hostilities. Discussions about what is okay and what is not would be easier if they focused purely on the activities themselves, rather than trying to pigeonhole cyber behaviors according to intent.

***