Cyber Espionage or Cyber Attack: Is the answer (a), (b) or (c) Both of the Above?

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. 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 so much a part of everyday life that its use 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 or escalation of tensions. It also discusses the US stand 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 on-line, have driven a closer look at the subject of cyber espionage, in particular the ways it differs from more 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.[1] Although some of the issues discussed here are also relevant in traditional cyber operations, they have seemed less **relevant** in the past. They may have come to the forefront now because of the effectiveness and pervasiveness of cyber espionage, and this article will focus on cyber methods of espionage.

The US 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."[2]

Cyber espionage presents special definitional issues. In the purely physical world it's 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's 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's often the intent of spies to look like insiders, or people who have permission to be where they are. Troops planning to engage

[1] Verizon's 2015 *Data Breach Investigations Report* notes that in 60% of cases, cyber operators are able to compromise a target organization within minutes, http://www.verizonenterprise.com/DBIR/2015/ (last accessed Jun. 11, 2015). The Sony hack resulted in around 100 terabytes of data being stolen, which is around seven times as much data as there is printed material in the Library of Congress. Much of Sony's data was audio and video, however, so the comparison is somewhat misleading, http://www.wired.com/2014/12/sony-hack-what-we-know/ (last accessed Jun. 11, 2015).

[2] JP 1-02 (8 Nov. 2010, as amended through 15 Nov. 2014). The offense is essentially the same under 18 U.S.C. § 794.

in combat, on the other hand, appear to be what they are – combatants.[3] They're 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.

In cyberspace, 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. 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's often not immediately apparent whether the unauthorized access is intended for spying or for disruptive or destructive activities (or both). The potential damage isn't 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 was espionage, having the access may give a future attacker an idea to use it in the future.

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. So, both quantitatively and qualitatively, espionage and warfighting in cyberspace can be indistinguishable until the denouement.

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 little result (beyond the imprisoned, executed or returned spy) other than exchanging the expulsion of diplomats. This is in stark contrast to the treatment of aggressive activity, which might constitute a use of force – expressly prohibited by the UN Charter.[5]

The US has generally seemed content with this permissive view of espionage, but recently seems to be modifying its position, firmly asserting that there is a distinction between the theft of trade secrets for the benefit of corporations and the theft of national security information for the benefit of states.[6] In February 2013, the cyber security

---

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

[4] Whether or not espionage is prohibited by international law doesn't affect whether it may be prohibited or otherwise regulated domestically.

[5] UN Charter, Art. 2(4).

[6] "Remarks by Assistant Attorney General for National Security John Carlin at a Brookings Institution Discussion," *Federal News Service*, Subject: "Tackling Emergency National Security Threats through Law

company Mandiant published a compelling portfolio of evidence tying the Chinese military to cyber economic espionage, at least tangentially supporting the US position that "economic espionage" should be treated differently than more traditional or "national security espionage."[7]

The US position that the cyber revolution has driven an increase in industrial espionage, and that this type of spying is fundamentally different than traditional espionage, is reflected in the indictments it brought against five members of the People's Liberation Army for pilfering confidential technological data from six US companies through cyber espionage.[8]

The US would treat as traditional espionage the theft of information more directly relevant to national security. "Traditional espionage encompasses a government's efforts to acquire clandestinely classified or otherwise protected information from a foreign government. Economic espionage involves a state's attempts to acquire covertly trade secrets held by foreign private enterprises."[9] The US 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]

There is logic in treating the theft of trade secrets differently than the theft of national security information. The latter 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. By contrast, economic espionage merely transfers net wealth and marginally decreases the

---

Enforcement," (May 22, 2014). See a discussion of the US position at Greg Austin, "China's Cyberespionage: The National Security Distinction and U.S. Diplomacy" (2015), http://thediplomat.com/wp-content/uploads/2015/05/thediplomat_2015-05-21_22-14-05.pdf (last accessed Jun. 11, 2015).

[7] *APT1: Exposing One of China's Cyber Espionage Units*, Mandiant, www.mandiant.com (18 Feb 2013).

[8] *US v. Wang Dong, et al*. (May 1, 2014), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor (last accessed Jun. 3, 2015). The *Economic Espionage Act*, 18 U.S.C. §§ 1831, 1832, defines both "economic espionage" and "industrial espionage." Industrial espionage is stealing trade secrets; economic espionage is undertaking the same activity for the benefit of a foreign government. This article will use the term "economic espionage" to mean a state spying to obtain information to be used by a private entity and "national security espionage" to mean all other espionage.

[9] David P. Fidler, "Economic Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies," *ASIL Insights* (Vol. 17, No. 10 (Mar. 20, 2013).

[10] Josh Rogin, "NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history,'" *Foreign Policy* (Jul. 9, 2012), http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/ (last accessed Jun. 11, 2015).

[11] The US Department of Commerce estimates intellectual property theft from US companies amounts to $200 to $250 billion annually. "Stolen Intellectual Property Harms American Businesses Says Acting Deputy Secretary Blank," *The Commerce Blog*, U.S. Department of Commerce (Nov. 29, 2011), http://www.commerce.gov/blog/2011/11/29/stolen-intellectual-property-harms-american-businessessays-acting-deputy-secretary- (last accessed Jun. 11, 2015).

incentive to innovate.[12] It might, then, make sense to treat economic espionage less favorably than more traditional espionage. Less favorable treatment might include official condemnation, responsive sanctions or the use of other international tools to dissuade economic espionage. To date, there has been no clear international consensus to single out economic espionage for denunciation.

Even if there were to be 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.[13] Rational arguments can be made for a vast array of technologies contributing to "national security." 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.[14]

Although the US is more 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. 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?

Merely gaining access to a network or computer system isn't a wrongful use of force or an armed attack under international law, but the *method* used might raise such questions.[15] Some cases are simple. It's easy to conclude that conducting an invasion of a military base located across a national border, causing hundreds of casualties, for the purpose of seizing a hard drive containing sensitive information isn't 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 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 demanding a meaningful response.

---

[12] Chistina Parajon Skinner, "An International Law Response to Economic Cyber Espionage," 46 CT. L. REV. 1165 (2014), p. 1183.

[13] It's frequently noted that China sees its economy and national security as two sides of the same coin. *See* http://time.com/105910/chinese-spying-economy-hacking-espionage/ (last accessed Jun. 11, 2015). The US *National Security Strategy* (2010) mentions aspects of the economy 50 times; it's clearly important to the US vision of national security, as well, https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (last accessed Jun. 11, 2015).

[14] *Commentary to Additional Protocol I*, para 1775, p. 566.

[15] *See* Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2013), Rule 66, commentary para. 9.

Even without the similarity to a ground attack, 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."[16] 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 includes decreasing effectiveness or causing a system to cease its intended function, then each of these is an illustration of damaging the targeted system.[17]

The potential overlap of espionage and offensive operations in cyberspace appears to have been recognized and has been addressed through policy and doctrinal definitions in the US. Cyber espionage is known 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."[18] The critical phrase is "enabling operations," which includes cyber activity that would otherwise be considered a cyber attack as noted above. "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.

Below, this article sets out a basic framework for analyzing cyber operations. It discusses the various phases of a cyber operation to illustrate the unique challenge of distinguishing between cyber espionage and aggressive cyber operations.

Before discussing the framework, there is one additional issue to address. Occupying the space between cyber espionage and cyber aggression is operational preparation of the environment (OPE). The Department of Defense defines OPE as "[t]he conduct of activities in likely or potential areas of operations to prepare and shape the operational environment."[19] OPE could include cyber operations to penetrate systems,

---

[16] William A. Owens, Kenneth W. Dam, & Herbert S. Lin, ed., "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities" (2009), p. 261.

[17] This concept of damage is also discussed below under Equation Group.

[18] Government Accountability Office memorandum, "Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates," (Jul. 29, 2011), p. 2.

[19] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Nov. 8, 2010, as amended through Mar. 15, 2015), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (last accessed Jun. 3, 2015).

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, doesn't constitute cyber aggression, and isn't quite espionage. This activity is rather some unique category falling between espionage and attack. What complicates the matter even more is that 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 as 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. It's mentioned here partly as an example of how easy it would be to mistake cyber intelligence operations for aggression.

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.

Put simply, any cyber operation requires identification, penetration, presence, exploitation and harm. We'll 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$z might do this by using a bot to conduct a massive survey of cyber systems, seeking out those with typical characteristics for the system he wants to target; for example, some SCADA systems have characteristics making them easy to spot on the Internet.[20] P0wn$z will be looking for the type of systems he wants that has +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.[21]

---

[20] ICS-CERT noted the ease of identifying some of these systems in *ICS-CERT Monitor* (Jan.-Apr. 2014), https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf (last accessed Jun. 8, 2015).

[21] Some of the methods used to identify vulnerable systems are set out in Pedram Hayati's, "Uncovering Secret Connections among Attackers by Using Network Theory and Custom Honeypots" (May 28, 2015), http://conference.hitb.org/hitbsecconf2015ams/materials/Whitepapers/Uncovering%20Secret%20Connections%20Among%20Attackers%20by%20Using%20Network%20Theory%20and%20Custom%20Honeypots.pdf (last accessed Jun. 8, 2015).

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, it was through a worm. In the case of Operation Buckshot Yankee[22], it was apparently 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. Whatever the method, the perpetrator uses it to gain and elevate access to the target system. That is, the idea 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 be able to access the system repeatedly, because not everything can be accomplished at once. To exfiltrate large amounts of data, P0wn$z will spread the downloads over the course of several days or weeks to avoid being caught by network monitoring tools. Besides, new information will be added to the system constantly, and a persistent access may yield results for many years. To establish persistent access, P0wn$z may install additional malware or create additional accounts on the system, for example, to provide a backdoor for future use.

The third 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 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 result is 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 US obtained access to the German Chancellor's cellphone.[23] The term "harm" as defined here includes changes in the relative advantage between states, because spying friends are

[22] See below.

[23] *Der Spiegel*, "Embassy Espionage: The NSA's Secret Spy Hub in Berlin" (Oct. 27, 2013), http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html (last accessed Jun. 8, 2015).

potential future adversaries. As Henry Kissinger famously noted, "America has no permanent friends or enemies, only interests."[24]

As noted earlier, the US sees a subset here. In the US view, using the pilfered information for commercial gain, rather than for advancing the national security of the state, is fundamentally different than using it for the advancement of national security.[25] China, however, has asserted that a state's economy is an essential part of its national security, so damaging one state's economy (e.g., the US) or benefiting the economy of another (e.g., China) is the same as any other use of information obtained through espionage.[26] Whether one position is superior in law won't be discussed here, it can be difficult to determine whether a particular operation is undertaken for the purpose of commercial gain or whether it merely 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 sought 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 identification is left for another paper.

Undersea Cable Tapping. Cable tapping is discussed as a cyber operation because most Internet traffic passes through submarine cables. The US has reportedly collected information from undersea communications cables for years. In the 1970s the US attached

---

[24] 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 Carera, *BBC*, "Spying scandal: Will the 'five eyes' club open up?" (Oct. 29, 2013), http://www.bbc.com/news/world-europe-24715168 (last accessed Jun. 8, 2015).

[25] Shannon Tiezzi, "China's Response to the US Cyber Espionage Charges," *The Diplomat* (May 21, 2014), http://thediplomat.com/2014/05/chinas-response-to-the-us-cyber-espionage-charges/ (last accessed Jun. 11, 2015).

[26] In the end, there may be little difference between the US and Chinese views on this matter, though the US 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* Administration Strategy on Mitigating the Theft of U.S. Trade Secrets (Feb. 2013), p. 3, https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf (last accessed Jun. 11, 2015).

recording boxes to Soviet undersea cables.[27] Later, the US (and others) may have tapped into submarine cables at repeater junctions under the sea.[28] From published reports, this appears to be a blended 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 apparently accomplished through a variety of physical means.[29] 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 US Cold War divers retrieving tapes from Soviet cables biweekly.[30]

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.

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 USCENTCOM's computer network, from where it spread across the military system, infecting both classified and unclassified computers. The 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.[31]

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. 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

---

[27] Olga Khazan, *Wired*, "The Creepy, Long-Standing Practice of Undersea Cable Tapping" (Jul. 16, 2013), http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/ (last accessed Jun. 11, 2015).
[28] *Id.*
[29] http://www.cnn.com/2014/03/04/tech/gallery/internet-undersea-cables/ (last accessed Jun. 11, 2015).
[30] Khazan.
[31] William Lynn & Nicholas Thompson, "Defending a New Domain," *Foreign Affairs* (Sep./Oct. 2010).

classified to the unclassified system. From the unclassified system, sensitive information could be transferred over the Internet.[32]

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.

F-35 Plans. Although few details haves been released, it has been reported that in 2007 China hacked US government contractor computer networks and obtained millions of pages of F-35 (also referred to as the Joint Strike Fighter or JSF) technical data.[33] "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.'"[34]

This may at first appear to be another typical espionage case, and perhaps it is. It also helps illuminate the complexity of applying the US position on good and bad espionage. US officials noted that the theft of this data caused great damage to US interests, giving away a substantial US advantage, while reducing the lead time and costs to adversaries working to develop stealth technology themselves.[35] The harm that resulted to the US 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, who presumably profited from it, all the while improving China's air force and national security.[36] Where is the line between strategic technology and more quotidian advances? It may be difficult to draw. Solar power? It could make troop deployments more efficient by reducing fuel needs. Automobile technology? Military vehicles might be improved with it. An advance in health sciences? Battlefield medicine might improve. Virtually any manufacturing technology can be related to national security.

---

[32] House Armed Services Subcommittee, Cyberspace Operations Testimony, General Keith Alexander Washington, D.C. (Sept. 23, 2010), http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/House%20Armed%20Services%20Subcommittee%20Cyberspace%20Operations%20Testimony%2020100923.pdf (last accessed Jun. 9, 2015).

[33] Nakashima, *Washington Post* (May 27, 2013), http://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 (last accessed Jun. 11, 2015).

[34] http://www.aero-news.net/index.cfm?do=main.textpost&id=d877e953-ae71-460b-948a-ca4a79249c17

[35] "China's Cyber-Theft Jet Fighter," *Wall Street Journal* (Nov. 12, 2014), http://www.wsj.com/articles/chinas-cyber-theft-jet-fighter-1415838777 (last accessed Jun. 11, 2015).

[36] http://en.wikipedia.org/wiki/Shenyang_Aircraft_Corporation#In_Development (last accessed Jun. 11, 2015).

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."[37]

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 capable of damaging the system directly, if you can't 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 isn't 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.[38]

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. SCADA systems are critical to 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 don't contain much information of interest, except to those who might be planning a cyber attack on the system. Because states don't 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.[39]

In this case, is it possible that merely establishing persistent *presence* on a SCADA system could be taken as aggressive? In most cases the intelligence value of any

---

[37] 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/ (last accessed Jun. 3, 2015).
[38] Goodin.
[39] John Hultquist, "Targeting SCADA Systems," *iSight Partners* (Oct. 21, 2014), http://www.isightpartners.com/2014/10/sandworm-team-targeting-scada-systems/ (last accessed Jun. 11, 2015).

information is so low that it might be assumed that the operation isn't an exercise in simple espionage, but rather a prelude to aggression. US SCADA systems are frequently the object of cyber operations.[40] The *harm* that could be done is considerable. In 2014, a hacker caused "massive damage" to a steel plant in Germany.[41]

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 was facilitated by computer credentials stolen from the company's air conditioning service provider. That incident resulted in the exposure of 70 million Target customers' personal data.[42] Thieves and military planners may have good reasons for hacking into SCADA systems – but spies remain problematic.

A final case that may help bring all the threads together is the Sony hack. The facts of the incident work well for this discussion if we substitute the FBI for Sony. The FBI might have detected the intruders at an early phase of the operation: penetrating the federal computer system, establishing a persistent presence or exfiltrating sensitive anti-terrorism data, for example. At any of these times, it would have appeared to be nothing more than an espionage case. Then, perhaps without warning, the operation turned aggressive. The same malware capabilities used to exfiltrate data were used to delete (destroy) data and to render much more inaccessible by corrupting the master boot records of hard drives.[43] Would such a virtual destruction of a critical government information system rise to a level justifying a kinetic response? The US 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."[44] 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?[45]

---

[40] Joel Langill, et al., "Cyberespionage Campaign Hits Energy Companies," *Security Matters* (Jul. 8, 2014) http://www.secmatters.com/sites/www.secmatters.com/files/documents/whitepaper_havex_US.pdf (last accessed Jun. 11, 2015).

[41] Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *Wired* (Jan. 18, 2015), http://www.wired.com/2015/01/german-steel-mill-hack-destruction/ (last accessed Jun. 11, 2015).

[42] Matthew 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 (last accessed Jun. 9, 2015).

[43] Deleting the master boot record of a hard drive makes it nearly impossible to access the data on the drive, even though it's still present.

[44] *International Strategy for Cyberspace* (2011), p. 14, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (last accessed Jun. 3, 2015).

[45] 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's an issue for another day.

CONCLUSION. Because the tactics and techniques used in espionage and military operations in cyberspace are often identical, there is great potential for international misunderstanding and miscalculation. This is the situation with which the international community must contend. Espionage will continue to be required as part of a responsible strategy before military action, and there is no indication the world's "second oldest profession" will end even in the absence of aggressive intent.

Despite the potential pitfalls set out here, states may generally be relied on to pursue the courses of action – in this case the cyber options – they think best serve their own interests. In a loosely governed environment like cyberspace, it's especially important to have a shared understanding of boundaries to avoid unnecessary tension, or even escalation to hostilities. A careful consideration of the distinct steps of both cyber spying and cyber military operations might be a first step to understanding where the lines might be drawn.