Brookings Institution Press

Chapter Title: Cyberwar Inc.: Examining the Role of Companies in Offensive Cyber Operations
Chapter Author(s): IRV LACHOW and TAYLOR GROSSMAN

Book Title: Bytes, Bombs, and Spies
Book Subtitle: The Strategic Dimensions of Offensive Cyber Operations
Book Editor(s): Herbert Lin, Amy Zegart
Published by: Brookings Institution Press. (2018)
Stable URL: https://www.jstor.org/stable/10.7864/j.ctv75d8hb.20

16

Cyberwar Inc.

Examining the Role of Companies in Offensive Cyber Operations

IRV LACHOW *and* TAYLOR GROSSMAN

The private sector is an important driving force behind the development of cybersecurity products and services. National governments are the hubs for the creation and use of offensive cyber capabilities, both because of legal constraints around the use of force and because warfighting is usually considered to be the province of nation-states. At the same time, the lines between industry and government are blurring. Private sector actors are becoming increasingly influential in the international arena and governments are relying on companies for assistance with offensive as well as defensive operations—a development with profound implications for both domestic politics and international relations. This chapter seeks to identify pressing issues associated with the growing role of private companies in supporting offensive cyber operations. Its goal is to inform policymakers of the challenges they face while

The authors would like to thank Matt Venhaus for his thorough review and helpful suggestions. Thanks also to Herbert Lin and Marion Michaud for their guidance and support.

laying out a research agenda that can guide the work of scholars and practitioners.

The chapter begins with a description of cyber operations to set the stage for the analysis that follows. It then explores three areas where companies are providing cyberattack capabilities to governments: intelligence, surveillance and reconnaissance; the development of cyber weapons; and planning and support. The chapter then examines the implications of this development both domestically and internationally. It closes by offering recommendations for future research.

Understanding Offensive Cyber Operations

There is much confusion around the use of terms such as “cyberattack” and “cyber operations.” For example, the word “cyberattack” is often applied to cyber espionage and cyber crime. According to the U.S. Department of Defense (DoD), “Cyber Operations” missions are categorized as offensive cyber operations (OCO), defensive cyber operations, and DoD information network operations based on their intent.[1] Offensive cyber operations, the primary focus of this chapter, are defined as “cyberspace operations intended to project power by the application of force in and through cyberspace.”[2] Offensive cyber operations have various direct effects that include denying, degrading, disrupting, destroying, or manipulating information, computer systems, or networks of an adversary.[3] This chapter uses the terms “offensive cyber operations” and “cyberattack” interchangeably with the understanding that they both refer to force projection in and through cyberspace for the purposes of degrading, disrupting, or destroying a particular target.

Cyber operations conducted by governments, like military operations in general, require extensive preparations. As Chris Inglis notes in chapter 2, intelligence, surveillance, and reconnaissance (ISR) and operational preparation of the environment play especially important roles in cyberspace. Trey Herr and Drew Herrick echo this point:

> Cyber-enabled ISR focuses on gathering information on a specific adversary’s systems, including their hardware/software configurations, personnel, and operational security. This information is critical for effective targeting, operational planning, and “weaponeering” or preparing capabilities to achieve their desired effects. Cyber [opera-

> tional preparation of the environment], for its part, focuses on access to a target system, and on the means of preparing it for the specific operation.[4]

The cyber kill-chain model is a useful construct for understanding the steps that an attacker must go through to launch a successful cyber operation. Developed by several experts from Lockheed Martin, the cyber kill-chain is defined as "a systematic process to target and engage an adversary to create desired effects."[5] Simply put, a cyber intrusion requires an aggressor to develop a payload, breach a trusted boundary, establish a presence within a trusted environment, and take actions within that environment. More specifically, the attacker must accomplish seven steps in the cyber kill-chain:

1. Reconnaissance. The attacker starts by researching, identifying, and selecting targets. Reconnaissance may also involve examining vulnerabilities and exploits for possible use in later steps of the kill-chain.

2. Weaponization. Malware is coupled with an exploit and payload to create a cyber weapon.

3. Delivery. This step consists of transmitting a weapon to its target. Delivery can be accomplished via several means, including phishing emails and the use of infected USB drives.

4. Exploitation. After the weapon has been delivered to the target system, code is activated that enables the weapon to take advantage of the particular exploit it was designed to use.

5. Installation. After the exploitation code has been run, the weapon installs the payload into the target system. The code is now embedded in the trusted environment, often without the defender knowing that this has occurred.

6. Command and Control. The installed code is inside the target system, and most often it will beacon back out to let the attacker know that it is in place. The attacker can then send instructions to the malware.

7. Actions on Objectives. The attacker is now in a position to take actions within the target environment. These actions could focus on denial, degradation, disruption, destruction, or manipulation of data.

The seven steps of the cyber kill-chain can be grouped into three broad phases: pre-launch, launch, and post-launch. The pre-launch phase includes intelligence gathering and reconnaissance, planning, weaponization, and testing. The second phase focuses on delivery of the weapon via a propagation method.[6] The third phase consists of post-intrusion activities: installation of the malware on the target system (which may involve lateral movement within the target network), command and control of the malware (which may involve the downloading of additional malware), and actions on objectives. The attacker may also attempt to assess the damage of the operation.[7]

Because of legal and practical considerations, contractor support for OCO will likely focus on the pre-launch phase. Even within this phase, there may be constraints on the specific activities that private sector actors can perform. In many countries, domestic laws preclude companies from being actively involved in gathering intelligence or launching cyberattacks. For example, in the United States, the Computer Fraud and Abuse Act prohibits companies and individuals from accessing computers (inside or outside the United States) without the authorization of the owner or operator of those systems. There may also be limits based on international law. For example, as Oona Hathaway and Rebecca Crootof write, “States may not employ civilian contractors to carry out activities where they will exercise discretion that implicates the law of armed conflict [LOAC].”[8] Thus, American companies cannot be directly involved in any “hands-on keyboards,” activities that would either violate the Computer Fraud and Abuse Act or LOAC. In practice, these laws may keep private sector actors from participating in actions that deliver a cyber weapon to a target or actions that involve delivering a malware payload for intelligence-gathering purposes.

Intelligence, Surveillance, and Reconnaissance

Intelligence, surveillance, and reconnaissance (ISR) are vital because cyberattacks are designed to penetrate particular networks and systems to create specific effects. As Paul Roberts writes, “The quality of the intelligence gathered on a particular target makes the difference between an effective cyber weapon and a flop.”[9] Private sector activities in this phase could include understanding and mapping target networks and systems, identifying vulnerabilities in those targets, and possibly even gaining information on users who might be targeted by spear phishing and other delivery mechanisms.

The type of detailed intelligence needed to support OCO used to be solely the province of government spy agencies, but that is no longer the case. Shane Harris notes, "This kind of intelligence used to be the near-exclusive domain of government intelligence agencies. They alone had the access and the know-how to sniff out vulnerable computers with such precision . . . not anymore."[10] A recent RAND study has determined that some signals intelligence capabilities which were previously limited to governments are now "available to anyone."[11] These capabilities go beyond the spyware that is often associated with cyber monitoring. The RAND report notes, for example, that one university researcher built a rudimentary cyber surveillance system for less than $900 in one week that had the following capabilities: bulk data collection, search, cookie tracking, anonymous user identification, and malware injection.[12] Although this system has nowhere near the capabilities of sophisticated state actors, its development does suggest that cyber capabilities are spreading rapidly, while the costs of acquiring them are decreasing.

It should not be surprising that there is a market of companies providing extremely sophisticated cyber intelligence services. For example, the following description is taken from FireEye's website:

> FireEye iSIGHT cyber threat intelligence is unique in the industry. Our team of more than 160 intel experts span the globe and apply decades of experience in intelligence collection and analysis to their work. With native speakers in over twenty languages, the FireEye iSIGHT Intelligence team has the cultural and colloquial knowledge required to understand important nuances discussed in the underground. We produce deep, rich, contextual intelligence that includes motivation, intent, targets, attribution and methods, plus threat and technical tags. The FireEye iSIGHT Intelligence team employs a formal intelligence process, similar to a state-based intelligence organization, but optimized over nearly a decade, to rapidly collect and analyze findings and disseminate new intelligence to customers.[13]

CrowdStrike, a FireEye competitor, offers similar capabilities, promising to provide "the latest insights and indicators of compromise from an all-source methodology of intelligence gathering, analysis, and dissemination." The company notes that its "global intelligence team gathers, analyzes, and reports on over ninety threat actors that operate around the world."[14] Notably, both FireEye and CrowdStrike focus on public sector as well as private sector customers. And while they market their capabilities for defensive purposes, the types of intelligence they and other cybersecurity firms provide could be useful for offensive cyber operations as well.

In the United States, cyber ISR capabilities may also be provided by cleared defense contractors—private entities "granted clearance by the Department of Defense to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of the Department of Defense."[15] There is an array of cleared defense contractors that provide a mix of cyber, intelligence, and operational capabilities to U.S. government sponsors.[16]

Finally, there are boutique firms that provide specific types of cyber intelligence that could be useful for OCO. For example, startups such as FlashPoint and Surfwatch Labs provide intelligence about the dark web—the hidden part of the World Wide Web that can only be accessed via specific applications and communications links. The following description of FlashPoint's capabilities focuses on cybersecurity, and yet one could easily imagine "actionable" intelligence being used to support offensive operations:

> Flashpoint illuminates the Deep and Dark Web. A pioneer in providing intelligence from these regions of the Internet, Flashpoint's software and data services help companies, governments, and consumers enhance their cyber and physical security. The company's unique blend of subject matter expertise and software engineering has changed the way meaningful and actionable intelligence is gleaned from the previously unmapped regions of the Internet.[17]

Weaponization

There is no single definition of a cyber weapon. For our purposes, it is useful to think about weaponization as the combination of three factors: a vulnerability, an exploit, and a propagation method. A vulnerability is a weakness or flaw in hardware or software that can be taken advantage of by an attacker. An exploit is code written to take advantage of a vulnerability to cause a specific effect, such as gaining access to a system or shutting down a piece of hardware.[18] In other words, vulnerabilities are properties inherent in the systems (hardware or software) that one seeks to "hack," while exploits are the programs written to take advantage of these weaknesses. A propagation method, finally, is how an exploit is delivered to a target, such as a phishing email.[19]

Weaponization depends on intelligence that has been gathered previously to identify and develop the most promising vulnerabilities, exploits, and propagation methods. Governments can receive private sector support in the weaponization process via several channels, most notably through markets.[20] Generally speaking, markets come in three types: white, gray, and black.[21] White markets focus on identifying vulnerabilities to improve cybersecurity. Those who operate in such markets turn over discovered vulnerabilities to the affected vendor or publicly announce their findings so that organizations can take steps to protect themselves. In gray markets, vulnerabilities and exploits are often kept private and sold to governments, militaries, or defense contractors for both offensive and defensive purposes. Black markets focus on providing vulnerabilities and exploits to criminal groups and other buyers who have illicit purposes.

Although governments understandably try to keep a low profile when it comes to purchasing vulnerabilities and exploits from the private sector, there is a growing body of evidence that such interactions are commonplace. For example, in 2015 a company called Hacking Team, which provides "surveillance and intrusion software," was breached and its records were made public, revealing that almost forty governments around the world had purchased their products.[22] Similarly, a recent profile of a startup from Australia called Azimuth Security claims that the company provides exploits to the "Five Eyes" countries: the United States, the United Kingdom, Canada, Australia, and New Zealand.[23] Finally, RAND has determined that "approximately two dozen companies are in the business of selling [exploits] to U.S. or U.S.-allied entities."[24]

There is also evidence that large government contractors may play a role in the development of cyber weapons. For example, a recent Request for Proposal from U.S. Cyber Command sought support for "the development, evaluation, analysis, and integration of cyber weapons/tools/capabilities."[25] This was part of a broader request for support that could only be provided by a large cleared defense contractor. This is discussed further in the next section. The key takeaway is that private sector actors play a role in providing governments with vulnerabilities and exploits that can support the development of cyber weapons.

Planning and Support

The previous discussion examined how private sector actors can support OCO by participating in the steps of the cyber kill-chain. Companies also help governments conduct cyberattacks by providing general support that enables such cyber operations to take place. For example, in the Request for Proposal described earlier, U.S. Cyber Command sought assistance in the following areas: operations, planning, training and exercises, strategy and policy, information technology, communications, business support, and engagement. These activities are important to the overall function of the Command, but they are not focused on operations per se.

It is likely that planning and general support for OCO will come from cleared defense contractors (or similar organizations in other countries). These companies work closely with the government across a range of functions, including cyber operations. They have a history of supporting the military, understand its culture, and usually have many employees with security clearances. Finally, there is the matter of scope. The ceiling of the U.S. Cyber Command solicitation is $460 million and requires the support of hundreds of people. This observation is supported by testimony from the former U.S. Cyber Command commander, Admiral Michael Rogers, before the Senate Armed Services Committee in which he noted that the 2016 U.S. Cyber Command budget had billets for 963 government employees (military and civilian) and 409 contract employees.[26] Small companies simply cannot provide that number of qualified and cleared personnel.

Although small companies can provide specialized services in specific areas, one would expect a large prime contractor to oversee the overall work program and provide the bulk of support services. In fact, this is exactly what happened in the U.S. Cyber Command solicitation described earlier in this chapter: KEYW Corporation; Vencore, Inc.; Booz Allen Hamilton, Inc.; Science Applications International Corporation; CACI, Inc. Federal; and Secure Mission Solutions, LLC[27] were all selected to support U.S. Cyber Command. Foreign governments likely rely on similar types of companies to support their versions of U.S. Cyber Command, especially if such government organizations are relatively large.

Implications

Private sector actors are playing an important role in supporting OCO, and that role is likely to grow. The implications of this trend affect both domestic policy and international relations. We discuss four key issues below: how offensive cyber operations may affect domestic work force shortages, oversight, international power dynamics, and the use of proxies.

Domestic Workforce Issues

Many arms of the U.S. government are using companies to fill staffing gaps across the spectrum of cyber support and operations. Private sector actors provide a crucial benefit by supporting staffing needs that cannot be satisfied through normal recruiting and hiring processes. The U.S government has been quite open about its challenge in hiring qualified cyber professionals. In 2018 a DHS official summed up this difficulty, stating, "It's really hard for us to maintain key people in cybersecurity areas when they could make maybe three or four times their salary in the government . . . it is a struggle for the government to keep good IT security people."[28]

Cyber workforce challenges are most acute for the armed services. The military faces greater hurdles in both finding and retaining highly skilled professionals than the intelligence community and other federal agencies do.[29] Notably, U.S. Cyber Command initially intended to build a workforce of six thousand cyber professionals by 2016 but was unable to meet this timeline and had to request delays.[30] In part to remedy this problem, the U.S. Army launched its own program to fill lingering workforce gaps.[31]

The skills shortage is relevant for OCO because these operations require intense levels of training to create cyber warriors who can develop and launch cyberattacks. Individuals with existing talent and training in this field are few and far between, and are usually courted by private sector companies. The federal government faces extreme challenges when competing with industry for top cybersecurity talent. As a *Politico* article put it in 2015, "if there's an employer less like the cash-rich, flex-time, playful ethos of Silicon Valley than the federal bureaucracy, it's hard to imagine what it is."[32]

Unfortunately for DoD and other agencies, the workforce problem is likely to get worse before it gets better. Even when the government can hire people into its ranks, retention remains a major challenge. The military may hire a young cyber analyst and train him or her at great expense to become a highly proficient cyber warrior, only to have that individual lured away by a private company after a few years of government service. Industry can offer higher salaries, the prospect of more rapid advancement, open working conditions, and stock options—perks that government agencies cannot match. Former NSA employees, one article noted, "are becoming a hot commodity in Silicon Valley . . . investors looking to ride the boom in cybersecurity are dangling big paydays in front of former NSA staffers, seeking to secure access to the insider knowledge they gained while working for the world's most elite surveillance agency."[33] The *Washington Post* has reported that the NSA has lost hundreds of hackers, engineers, and data scientists in just the last few years. According to government officials, "the potential impact on national security is significant."[34]

If the military cannot hire enough cyber warriors on its own, it may find itself in a position where it has no choice but to rely on contracting private sector actors to conduct OCO. There is a vast difference between *choosing* to use the private sector and *needing* to use the private sector. The latter situation raises important concerns of oversight; for example, the federal government may be forced to rely on contractors for exceedingly sensitive support roles, or even employ contractors that it may feel are not up to the task.

Oversight Issues

If the U.S. government employs a growing number of private sector actors for OCO, oversight issues may become increasingly challenging. Government contracting officers need to have a mix of subject matter expertise, contracting know-how, and general experience to properly manage cyber-related contracts to ensure that they are being carried out effectively, ethically, and legally. A contracting officer plays an enormous role in overseeing agreements between private sector actors and contracting agencies, providing "technical direction, clarification, and guidance with respect to the contract specifications and statement of work. The contracting officer is the technical liaison between the government and industry and is responsible for ensuring satisfactory performance and timely delivery as set forth in the contract."[35] This kind of expertise is not easy to develop, and the military must ensure it has enough specialists of high caliber to oversee the large number of contracts it is granting.

Precedent for concern exists here. The U.S. government, including both the DoD and the State Department, had major problems overseeing private military contractors during the Iraq and Afghanistan conflicts. Several reforms were implemented by both the executive branch and Congress, and the number of contracting and acquisition personnel was also greatly expanded.[36] However, cyber operations contracts may pose a unique challenge owing to their scope, complexity, and level of classification. Given the shortage of cyber expertise in the federal government, and the growing reliance on private sector actors to fill these gaps, it is possible that there will not be enough qualified contracting officers to effectively oversee contracts involving OCO.

This potential shortage could lead to two acute risks, one financial and the other operational.[37] The financial risk is straightforward: a lack of contract oversight could result in contractor fraud, waste, and abuse. Fraud was perpetrated by contractors in Iraq and Afghanistan, and has also occurred on many major contracts involving weapons systems and information technology. By one estimate, contract waste and fraud amounted to between $31 billion and $60 billion in the Iraq and Afghanistan engagements.[38]

The operational concern is a bit trickier. Cyber contractors could conceivably take actions that have international or strategic implications. Such an issue arose during the Iraq War, when the United States became embroiled in a controversy later known as the Nisour Square Massacre. Four employees of Blackwater, a private military contractor, were eventually convicted in federal court of killing fourteen unarmed civilians, and U.S.–Iraq relations were severely strained as a result. The legal battle over these Blackwater employees has only become more complicated over time.[39] While the chances of a "cyber Blackwater" event may be low, the consequences of such an occurrence could be significant.

Even if the U.S. government can oversee its contractors effectively, the government still has limited control over the business decisions that such firms make. A few laws and regulations are in place to limit undesirable outcomes, such as export controls around the transfer of certain specified technologies.[40] U.S. military contractors also want to avoid making business decisions that upset their government customers. Yet ultimately, these companies have a great deal of leverage in deciding whom they support and how. As Peter Singer writes, "The simple fact is that there are no guarantees over where or for whom the firms will work."[41] A private sector actor could conceivably conduct an offensive cyber operation outside the purview of any government. In addition, a company that decided to develop and sell the ability to conduct sophisticated and comprehensive cyberattacks could prove to be a wildcard in the international arena. Finally, the use of contractors may increase the risk that an insider will inadvertently or deliberately leak sensitive information.[42]

International Balance-of-Power Issues

Companies already provide advanced cyberattack capabilities to customers around the globe. This reality may have international implications. Singer writes that the privatized military industry creates "alternative patterns of power and authority linked to the global market, rather than limited by the territorial state."[43] These patterns, in turn, unavoidably affect domestic politics and international dynamics. The proliferation of private sector actors in OCO raises a key question about global power dynamics: Will private sectors actors level the playing field for offensive cyber operations or exacerbate the gaps between the haves and the have-nots?

Whether and how private sector actors will affect power differentials in cyberspace is widely debated among academics and practitioners. On the one hand, the availability of cyber know-how could level the playing field between countries. An expanded market of offensive cyber capabilities could make it more economically feasible for countries with limited in-house cyber capabilities to acquire and launch OCO.[44] Alternatively, the use of private sector actors could accentuate the gap between haves and have-nots in cyberspace. As discussed earlier, conducting OCO requires a wide range of supporting actions as well as some level of direction and oversight. Although companies can provide many of the capabilities needed to launch a sophisticated cyberattack, these capabilities must be embedded into a broader strategy and military structure to achieve desired results beyond simply sowing chaos. It is easy to acquire sophisticated cyber crime tools and to utilize "malware as a service" to avoid the need to build and maintain a large internal infrastructure for malware creation.[45] However, OCO that is part of a sustained strategic campaign requires additional support. For example, because cyberspace is a complex domain with rapidly changing technical features, cyber weapons require detailed and timely intelligence about the intended target.

Given these considerations, it may be difficult for a country with limited cyber resources and infrastructure to simply buy an off-the-shelf offensive capability from a private sector actor and effectively operationalize it to align with full-scale military operations. Actors attempting to base their entire cyber arsenal on market-available tools and services would look more like sophisticated cyber criminals than powerful nation-states. These countries would not be able to keep up with advanced players already possessing sophisticated internal capabilities. A more powerful state can easily acquire the same readily available off-the-shelf tool or service as the cyber novice.

Yet, where the novice has to rely solely on the ready-made tool, the expert can integrate it into existing capabilities to build a much more effective campaign.

In addition, the involvement of government players in the exploitation marketplace may drive up the prices for zero-day vulnerabilities, essentially forcing out poorer or less powerful countries from these kinds of exchanges. Wealthier countries tend to have more advanced cyber infrastructures and can afford to invest beyond defensive capabilities and into the offense-oriented realm: "The market for back-door exploits has been boosted in large part by the burgeoning demand from militaries eager to develop their cyber war-fighting capabilities . . . [and] the U.S. military's dominant presence in the market means that other possible purchasers cannot match the military's price."[46] This is yet another example of how private sector actors may exacerbate power differentials in cyberspace.

Private Sector Actors as Combatants

As private sector actors play an increasingly active role in enabling and supporting OCO, their status in conflict becomes murkier. Can states legitimately treat contracted private sector actors as combatants in cyber conflict under international law? In general, civilians are not legitimate targets in a military conflict. However, civilians can lose that protection if they directly participate in hostilities or act "in a continuous combat function."[47]

> The civilian designer of a weapons system has traditionally not been treated as a direct participant in hostilities. However, the programmer who works with military intelligence may tweak the code to enable the attack, right up until the moment of the attack. The actions of such a civilian—particularly of a civilian who regularly engages in such activity—could be considered a "continuous function [that] involves the preparation, execution, or command of acts or operations amounting to direct participation in hostilities." As a result, *civilians involved in cyber-attacks might be regarded as performing tasks that alter their status under the law of war, rendering them lawful targets of a counterattack.*[48]

To parse out the legal status of private sector contractors, one must determine whether the type of support provided by the actor can be considered direct participation in hostilities or a continuous combat function. Based on our earlier examination of the roles inhabited by the private sector in supporting OCO, these actors appear to be primarily focused on providing support activities before the launch of a cyber weapon. Even if those activities include intelligence gathering and military planning, private sector actors probably should not be viewed as legitimate targets for attack under the law of armed conflict.

However, this question cannot be put to rest quite so easily; it involves several legal, ethical, and practical considerations. For example, the majority of OCO will likely occur over the internet, which means that they will transit networks that are owned and operated by internet service providers (ISPs). What responsibility do ISPs have to identify and prevent such attacks from occurring? Could a country that suffers a cyberattack hold an ISP responsible, or view it as a legitimate target for retaliatory action? Do the answers to these questions differ from peacetime to wartime? The legal considerations surrounding contractor actions in cyberspace deserve continuing attention, especially as the role of companies continues to grow in both offensive and defensive cyber operations.

Further muddying the waters is the possibility that private sector actors could support both the offensive and defensive sides of a given operation. This occurrence is hardly a new phenomenon in warfare: hired hands have been fighting each other for hundreds of years. However, we have yet to fully understand the implications of this wrinkle in a cyber conflict featuring two cyber contractors facing off against each other in support of their respective government customers. One could imagine three scenarios with differing dynamics.

In the first scenario, a U.S.-based private sector actor supporting OCO might confront a foreign company that was hired to defend the organization that the operation is targeting. This situation is likely to occur because non-U.S.-based companies are becoming increasingly sophisticated and popular providers of cybersecurity products and services, even in the United States. Many countries are investing in home-grown cybersecurity markets, and several of these companies are known to be quite capable (for example, F-Secure of Finland, Kaspersky Lab of Russia, and Check Point Software Technologies of Israel).

A second scenario involves a U.S.-based private sector contractor facing off with another U.S. company. This situation is also quite likely as the United States boasts the world's largest and strongest market for cybersecurity services and products. In this situation, one company might need to find and exploit vulnerabilities in the software of another U.S. company to successfully penetrate the target's computer systems. If one company identifies vulnerabilities in another company's software or hardware, does it disclose that information to improve the security of all users? Or, does it choose to keep the information quiet so that it can succeed in its offensive mission?

A third and final scenario involves a U.S.-based private sector company becoming embroiled in both ends of an operation. This case is theoretically possible because some global defense contractors provide support to both offensive and defensive operations. A single company might support an OCO launched by the United States, while simultaneously providing defensive support to countries around the globe—including the target country of that same initial OCO. For example, the consulting firm Booz Allen Hamilton is known to support the NSA[49] and provide cybersecurity services to countries in the Middle East.[50] This situation is more likely to arise in the case of a cyber exploitation than a cyberattack. However, this scenario does raise interesting questions about the preeminence of offense versus defense, and the choices that companies may be required to make as they consider involvement both with the U.S. government and with governments abroad.

The position of private sector actors in cyber conflict is already complicated in the best of circumstances. In countries like the United States, private sector actors usually serve in well-scoped roles, as contractors who provide discrete support services. In many other countries, however, private sector actors operate in much murkier roles of "proxies." A nation-state may choose to hide its activities in the guise of a nonstate actor to avoid retaliation or to maintain its ability to engage in other realms (diplomatic, economic) without acknowledging its hand in OCO. China uses a wide range of actors to conduct cyber espionage: "The Chinese government created a proxy hacking system precisely so that it could deny state involvement."[51] The Russian government relies on criminals to gather information and launch attacks on its behalf.[52] Russia also encourages hacktivist groups to take actions on behalf of the state—a practice that dates back to the 2007 cyberattacks against Estonia.[53] Finally, it appears that Iran is growing increasingly reliant on proxies to augment its national cyber capabilities.[54]

By relying on proxies, a country may be able to create at least *some* confusion as to its involvement with an OCO by shifting most of the blame to a nonstate actor, while still (potentially) achieving its larger offensive goals. This kind of subterfuge raises a host of questions related to a broader cybersecurity debate: the role (and certainty) of attribution. A state that sanctions or sponsors a cyberattack may be able to avoid retaliation for its actions if attribution of such an operation remains uncertain.

Avenues for Future Research

Based on our findings, four avenues for research appear to be most promising and useful for policymakers. First, more attention needs to be paid to understanding how countries can balance the benefits and risks of reliance on private sector cyber capabilities. This area of research touches on topics such as recruitment and retention of cyber warriors, oversight for cyber contractors, and the role of cyber contractors in cyber conflict. Much work has been done to address a potential shortfall in cyber warriors.[55] However, most of the attention so far has focused on cyber defense. For example, The National Institutes of Standards and Technology has developed a detailed guideline on cybersecurity education.[56] More research is needed on how to attract and retain people who work on offensive cyber operations. A good first step would be a broader discussion around the magnitude of the problem, which is often shrouded in secrecy.

Additionally, the U.S. government needs to determine if there is a shortage of skilled contracting officers to oversee complex cyber projects, especially those involving offensive cyber operations. If there is a shortage, then steps should be taken to address that shortfall as soon as possible while putting in place a long-term plan for increasing the ranks of cyber-savvy contracting officers.

Second, developing a better understanding of state interests in and capabilities for OCO will shed useful light on whether, how much, and in which ways key states are likely to use private sector actors for such operations. For example, one could posit that the internal political landscape of countries will affect their willingness to engage in OCO. It is also important to explore whether the proliferation of cyber weapons and capabilities, partially abetted by the private sector, will level the playing field or exacerbate the gap between top tier and second tier cyber powers.

A related topic for exploration is determining whether the proliferation of cyber capabilities via private sector actors will increase or decrease global stability. It may be that global stability can be maximized by having a more equitable distribution of cyber capabilities. On the other hand, global stability may be improved by having a few dominant powers that "rule the roost." When one considers the impact of the private sector on both the global balance of cyber power and the stability of resulting power dynamics, four scenarios can be imagined. In the first scenario, a greater number of states develop offensive cyber capabilities, which leads to a more level playing field and greater stability. In the second scenario, the wide distribution of OCO capabilities evens out the distribution of power but ultimately leads to greater instability due to a lack of deterrence. The third scenario involves a world in which cyber restraint and stability reign even as the gap increases between cyber haves and have-nots. The fourth and final scenario features an unstable world where a few cyber powers dominate the playing field. This area is ripe for further research.

Finally, although there is a growing line of research examining the role that proxies can play in cyber conflict, more work needs to be done on how to distinguish between legitimate and illegitimate use of nongovernment actors to support cyber operations.[57] For example, is it acceptable for the United States to rely on cleared defense contractors but not acceptable for other countries to use proxies for their operations? What distinguishes the two? Is it a matter of attribution or command and control? What does international humanitarian law have to say about these issues? Should norms be developed, and if so, how can they be acceptable to the key players in the global arena?

Conclusion

There is a subtle but important change occurring in the cyber landscape: private sector actors are increasingly influential in protecting computer systems, and they are also beginning to affect the full range of both defensive and offensive cyber operations. As Jason Healey testified before Congress, "America's cyber power is not focused at Fort Meade with NSA and U.S. Cyber Command. The center of U.S. cyber power is instead in Silicon Valley, in Route 128 in Boston, in Redmond, Washington, and in all of our districts where Americans are creating and maintaining cyberspace."[58]

If current workforce and investment trends are indicators of what is to come, private sector actors will continue to grow in sophistication and will likely take on larger roles in offensive cyber operations. Understanding the implications of this development will be critical for both government and industry.

Notes

1. U.S. Department of Defense, *Cyberspace Operations*, Joint Publication 3-12 (R) (Washington, February 5, 2013).

2. Ibid.

3. Ibid. This definition is similar to the concept of a "cyberattack" used in the National Academy of Sciences report on offensive cyber operations: "'cyberattack' refers to the use of deliberate actions and operations—perhaps over an extended period of time—to alter, disrupt, deceive, degrade or destroy adversary computer systems or networks of the information and (or) programs resident in or transiting these systems or networks. Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law and Policy* 4, no. 1 (2010), pp. 63–86, at 63.

4. Trey Herr and Drew Herrick, "Understanding Military Cyber Operations," in *Cyber Insecurity: Navigating the Perils of the Next Information Age*, edited by Richard M. Harrison and Trey Herr (London: Rowman & Littlefield, 2016), p. 261.

5. E. M. Huchins, M. J. Cloppert, and R. M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains* (Bethesda, MD: Lockheed Martin, 2011).

6. Trey Herr, *PrEP: A Framework for Malware & Cyber Weapons*, Report GW-CSPRI-2014-2 (Washington: George Washington University, 2014).

7. See Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations* (Oxford University Press, 2017).

8. Oona A. Hathaway and Rebecca Crootof, "The Law of Cyberattack," Faculty Scholarship Series 3852 (Yale University, 2012) (digitalcommons.law.yale.edu/fss_papers/3852).

9. Paul F. Roberts, "If This Is Cyberwar, Where Are All the Cyberweapons?," *MIT Technology Review*, January 27, 2014 (www.technologyreview.com/s/523931/if-this-is-cyberwar-where-are-all-the-cyberweapons/).

10. Shane Harris, *@War: The Rise of the Military-Internet Complex* (Boston: Houghton Mifflin Harcourt, 2014).

11. Cortney Weinbaum, Steven Berner, and Bruce McClintock, *SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain* (Santa Monica, Calif.: RAND, 2017).

12. Ibid., p. 7.

13. See FireEye, "iSIGHT Intelligence: The Details" (www.fireeye.com/products/isight-cyber-threat-intelligence-subscriptions/isight-intelligence-details.html).

14. See CrowdStrike, "Cyber Threat Intelligence Solutions," 2018 (www.crowdstrike.com/solutions/threat-intelligence-solutions/).

15. See IT Law Wiki, "Cleared Defense Contractor," 2016 (itlaw.wikia.com/wiki/Cleared_defense_contractor).

16. Dana Priest and William Arkin, *Top Secret America: The Rise of the New American Security State* (New York: Little, Brown, 2011).

17. See Threat Connect, "Flashpoint," 2018 (www.threatconnect.com/partners/flashpoint-intelligence/).

18. Herr, *PrEP*.

19. Ibid.

20. The RAND Corporation has conducted two studies about the nature of these markets, and their findings have provided some light. One key finding is that "any serious attacker can likely get an affordable zero-day for almost any target." Lillian Ablon and Timothy Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits* (Santa Monica, Calif.: RAND, 2017). See also Lillian Albon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (Santa Monica, Calif.: RAND, 2014).

21. Ablon and Bogart, *Zero Days, Thousands of Nights*.

22. Joseph Cox, “The FBI Spent $775K on Hacking Team’s Spy Tools since 2011,” *Wired*, July 6, 2015 (www.wired.com/2015/07/fbi-spent-775k-hacking-teams-spy-tools-since-2011/).

23. Joseph Cox and Lorenzo Franceschi-Bicchierai, “How a Tiny Startup Became the Most Important Hacking Shop You’ve Never Heard Of,” *Motherboard*, February 7, 2018 (motherboard.vice.com/en_us/article/8xdayg/iphone-zero-days-inside-azimuth-security).

24. Ablon and Bogart, *Zero Days, Thousands of Nights*, p. 25.

25. U.S. Cyber Command, *Attachment E, Seed Task Order 1 (TO1) for Cyberspace Operations Support Services*, GSC-QF0B-15-32959 (2016).

26. Senate Armed Services Committee, *Statement of Admiral Michael S. Rogers, Commander of the United States Cyber Command, before the Senate Armed Services Committee*, April 5, 2016.

27. Aaron Boyd, “CYBERCOM Awards Spots on New $460M Cyber Operations Contract,” *Federal Times*, May 23, 2016 (www.federaltimes.com/2016/05/23/cybercom-awards-spots-on-new-460m-cyber-operations-contract/).

28. “Unfilled Cyber Positions in Government Continuing to Increase, DHS Official Says,” *Inside Cybersecurity*, January 26, 2018 (insidecybersecurity.com/daily-briefs/unfilled-cyber-positions-government-continuing-increase-dhs-official-says).

29. David Barno and Nora Bensahel, “Can the US Military Halt its Brain Drain?,” *The Atlantic*, November 5, 2015 (www.theatlantic.com/politics/archive/2015/11/us-military-tries-halt-brain-drain/413965/).

30. Ian Duncan, “Lawmakers Push to Make U.S. Cyber Command a Top Military Command,” *Baltimore Sun*, May 22, 2016 (www.baltimoresun.com/news/maryland/politics/bs-md-cyber-command-combatant-command-20160522-story.html).

31. Morgan Chalfant, “Army Leaders Launch Program to Recruit More Cyber Warriors,” *The Hill*, December 5, 2017 (thehill.com/policy/cybersecurity/363349-army-leaders-launch-program-to-recruit-more-cyber-warriors).

32. Darren Samuelsohn,“Inside the NSA’s Hunt for Hackers,” *Politico*, December 9, 2015 (www.politico.com/agenda/story/2015/12/federal-government-cyber-security-technology-worker-recruiting-000330).

33. Cory Bennett, “NSA Staffers Rake in Silicon Valley Cash,” *The Hill*, February 24, 2015 (thehill.com/policy/cybersecurity/233740-nsa-staffers-rake-in-silicon-valley-cash).

34. Ellen Nakashima and Aaron Gregg, “NSA’s Top Talent Is Leaving Because of Low Pay, Slumping Morale and Unpopular Reorganization,” *Washington Post*, January 2, 2018 (www.washingtonpost.com/world/national-security/the-nsas-top-talent-is-leaving-because-of-low-pay-and-battered-morale/2018/01/02/ff19f0c6-ec04-11e7-9f92-10a2203f6c8d_story.html?utm_term=.f1c915ccae61).

35. See U.S. Army Medical Research Acquisition Activity, “Contracting Officer’s Representative (COR) Program,” 2016 (www.usamraa.army.mil/Pages/Cor.aspx).

36. Moshe Schwartz and Jennifer Church, “Department of Defense’s Use of Contractors to Support Military Operations: Background, Analysis, and Issues for Congress” (Congressional Research Service, May 17, 2013).

37. Ibid.

38. Ibid., p. 8.

39. Scott Neuman, “U.S. Appeals Court Tosses Ex-Blackwater Guard’s Conviction in 2007 Baghdad Massacre,” NPR, August 4, 2017 (www.npr.org/sections/thetwo-ay/2017

/08/04/541616598/u-s-appeals-court-tosses-conviction-of-ex-blackwater-guard-in-2007-baghdad-mass).

40. See U.S. State Department Directorate of Defense Trade Controls, "The International Traffic in Arms Regulations (ITAR)" (www.pmddtc.state.gov/regulations_laws/itar.html).

41. Peter Singer, *Corporate Warriors: The Rise of the Private Military Industry* (Cornell University Press, 2003).

42. Although the Snowden case is the best-known example of this phenomenon, it occurs with alarming frequency. For example, see Evan Perez, Jim Sciutto, and Laura Jarrett, "Contractor Charged with Leaking Classified NSA Info on Russian Hacking," CNN, June 6, 2017 (www.cnn.com/2017/06/05/politics/federal-contractor-leak-prosecution/index.html).

43. Singer, *Corporate Warriors*, p. 170.

44. Nicola Whiting, "Cyberspace Triggers a New Kind of Arms Race," *Signal*, February 1, 2018 (www.afcea.org/content/cyberspace-triggers-new-kind-arms-race).

45. Danny Palmer, "Criminals in the Cloud: How Malware-as-a-Service Is Becoming the Tool of Choice for Crooks," *ZDNet*, April 21, 2016 (www.zdnet.com/article/criminals-in-the-cloud-how-malware-as-a-service-is-becoming-the-tool-of-choice-for-crooks/).

46. Tom Gjelten, "First Strike: U.S. Cyber Warriors Seize the Offensive," *World Affairs Journal*, January/February 2013 (www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive).

47. U.S. Cyber Command, *Attachment E, Seed Task Order 1 (TO1).*

48. Hathaway and Crootof, "The Law of Cyberattack"; emphasis added.

49. Drake Bennett and Michael Riley, "Booz Allen, the World's Most Profitable Spy Organization," *Bloomberg Businessweek*, June 21, 2013 (www.bloomberg.com/news/articles/2013-06-20/booz-allen-the-worlds-most-profitable-spy-organization).

50. See Booz Allen Hamilton, "Booz Allen Hamilton to Support Business and Economic Growth in the Kingdom of Saudi Arabia," February 18, 2013 (investors.boozallen.com/releasedetail.cfm?releaseid=749160).

51. Ethan Gutmann, "Hacker Nation: China's Cyber Assault," *World Affairs* 173, no. 1 (2010), pp. 70–79.

52. Brian Whitmore, "Organized Crime Is Now a Major Element of Russian Statecraft," *Business Insider*, October 27, 2015 (www.businessinsider.com/organized-crime-is-now-a-major-element-of-russia-statecraft-2015-10).

53. Tim Maurer, "Cyber Proxies and Crisis in Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine*, edited by K. Geers (Tallinn: NATO CCD COE Publications, 2015), pp. 79–86.

54. Jordan Brunner, "Iran Has Built an Army of Cyber Proxies," *The Tower*, August 2015 (www.thetower.org/article/iran-has-built-an-army-of-cyber-proxies/).

55. Two examples of this: Franklin S. Reeder and Katrina Timlin, *Recruiting and Retaining Cybersecurity Ninjas* (Washington: Center for Strategic and International Studies, October 2016); and Center for Strategic and International Studies, *Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills* (Washington: McAfee, July 2016).

56. See William Newhouse, Stephanie Keith, Benjamin Scribner, and Greg Witte, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," NIST Special Publication 800-181 (Washington: National Institute of Standards and Technology, 2017).

57. For a comprehensive discussion of this topic, see Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge University Press, 2018).

58. U.S. Congress, House of Representatives, Armed Services Committee, *Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities—Testimony by Jason Healey*, 115th Cong., March 1, 2017.