Private Sector Cyberweapons:

An Adequate Response to the Sovereignty Gap?

[Revised.]

Lucas Kello, Oxford University

ABSTRACT. The cyber domain exhibits a sovereignty gap: the government cannot protect the private sector against all relevant threats. The challenge of cybersecurity, therefore, is essentially one of *civil defense*: how to equip the private sector to protect its own computer systems in the absence of decisive government involvement. Ordinarily, civil defense has involved passive measures such as resilience and redundancy. These measures, however, will not redress the sovereignty gap unless they are complemented by a proactive approach – especially the techniques of "active defense," which attempt to neutralize threats before they are carried out. Yet presently the authority to implement active defense belongs exclusively to the government. Top officials in the United States and other countries have called for changes in law and policy that would bolster private sector active defense, such the insertion of web beacons in hostile machines. This paper explores the possible strategic and other consequences of arming the civilian quarters of cyberspace with active defense capabilities. It argues that while the potential defensive and other benefits of private-sector arms are significant, the risks to defenders, innocent third parties, and international conflict stability are notably greater. Cyber civil defense should remain a reactive enterprise.

The Sovereignty Gap

The goal of national security policy is to preserve the safety of the state and its subjects against threats arising from other states. The organizing principle of international anarchy is that states are the supreme agents in this program of activity: they possess sovereign resources to carry out their own security policies against each other in the absence of world government. These are two classical tenets of international security studies; the central trends of cybersecurity challenge them. Whereas previously the main question of security policy was: What actions of other independent states threaten vital national interests? this is increasingly supplanted by the concern: How do forces operating outside state confines imperil the nation? States to be sure retain their primacy. Nevertheless, new entrants on the international scene – hacktivists, criminal syndicates, militant groups, firms, and so on – can inflict great harm in cyberspace. Security policy now has to be conducted against and by not only states but also a growing universe of other players of unclear origin and identity.

The gradual flight of power away from state structures has produced a sovereignty gap: the private sector can no longer take for granted the ability of the government to protect it against all relevant threats – if sovereignty means not just an interstate condition, i.e., the state is subject to no other state in the ordering of its internal affairs, as international law commonly defines the notion,[1] but one also involving freedom from the interference of unaffiliated actors. A U.S.-based oil firm may reasonably expect that the U.S. military will be able to prevent the seizure of its property by pirate vessels in the Persian Gulf,

[1] Wimbledon Case, Permanent Court of International Justice, A 1 (1923).

but it may not have much confidence that the government can fend off sophisticated criminals seeking to capture or damage prized assets in cyberspace.[2] Offense superiority in the new domain widens the sovereignty gap. Because of enormous defense complications, the government is even less able to defend private subjects against "advanced persistent threats," or adversaries that are able to penetrate home defenses continuously and surreptitiously (think of China or Russia), than against private culprits (such as political or ideological militants). A remark by the chief of Cyber Command General Keith Alexander, referring to a hypothetical cyber threat against Wall Street, conveys the problem: "[The] NSA and Cyber Command would probably not see it. We have no capability there."[3] A comment by John Chambers, the former executive chairman and CEO of Cisco Systems, captures the private sector's defensive agony: "There are two kinds of companies: those who have been breached and those who don't know they've been breached."[4] A further complication of the new domain is the confluence of criminal and national security activity, a blurring of the lines between hostile actions such as disruption of corporate functions that once implicated only private interests but which increasingly impinge on national security. As Joel Brenner puts it: "The boundary between economic and national security is also eroding – has eroded, in fact, almost

[2] The threat of piracy, however, has grown recently. The shipping industry has reacted by increasing the presence of armed security personnel onboard. M.N. Murphy, "Contemporary Piracy and Maritime Terrorism: The Threat to International Security," Adelphi Paper (2007), p. 388. P. Chalk, *The Maritime Dimension of International Security: Terrorism, Piracy, and Challenges for the United States* (Santa Monica: RAND, 2008).

[3] David E. Sanger, "NSA Director Says Snowden Leaks Hamper Efforts Against Cyberattacks," *New York Times* (March 4, 2014).

[4] Joseph Muniz, "Responding to Real-World Cyber Threats," Ciscopress.com (February 16, 2016).

completely."[5] The ideal-types of "public" and "private" goods and actors, in short, are merging in ways that the conventional science of international relations is unaccustomed – possibly unequipped – to decipher.[6]

The challenge of cybersecurity, therefore, is essentially one of civil defense: how to equip the private sector to protect its own computer terrain in the absence of decisive government involvement.[7] Ordinarily, civil defense in the new domain has involved passive measures, such as resilience and redundancy, which aim to harden defenses and deflect offensive hits. But foiling a sophisticated offensive operation that is already in train is very difficult to do, particularly if deep exploitation of the target networks preceded the attack.[8] Denial of the adversary's arms has a higher chance of success if it occurs before they reach the defending line. Passive measures, therefore, will not redress the defensive gap unless they are complemented by a proactive approach – especially the techniques of "active defense," or offense-as-defense, which attempt to neutralize external threats before they are carried out. As a senior official in the British Cabinet Office put it: "Successful defense requires making life harder for the enemy." It demands a posture of aggressiveness: "We're not going to just sit there and let you get us – we will go after you in cyberspace and

---

[5] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (London: Penguin, 2011), p. 13.

[6] The question of the salience of nonstate actors in international relations is not new. International relations theorists recognize the existence of nonstate actors. In Kenneth Waltz's words: "[S]tates are not and never have been the only international actors… The importance of nonstate actors and the extent of transnational activities are obvious." Kenneth N. Waltz, *Theory of International Relations* (New York: McGraw-Hill, 1979), pp. 93-4. But mainstream thinkers argue that states are so important as to be the central – some say only – units of analysis.

[7] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* Vol. 38 (2013), p. 29.

[8] This is often the case: for example, the handlers of the Stuxnet worm that hit the Natanz nuclear facility in Iran in 2009 may have compromised the industrial controller several years earlier. See David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown, 2012), Chapter 8.

make your life more difficult. This is why one sees offensive actions."[9] Yet presently in the United States and Britain, as in many other jurisdictions, the authority to implement active defenses belongs exclusively to the government. Top U.S. officials have called for changes in U.S. law and policy that would bolster the private sector's use of active defenses such as "strikeback" or "hackback" technology: in effect, arming of the civilian quarters of cyberspace.[10] The main body of government opinion has successfully resisted these calls – so far.

This paper asks: What are the possible strategic and other consequences of enabling the private sector to arm itself with active defenses? Little or no systematic analysis of this question exists. The paper argues that while the potential defensive and other benefits of private-sector arms are significant, the risks to defenders, innocent parties, and international conflict stability are notably greater.

But first, a clarification of key terms is in order. The label "private sector" in this paper denotes the entirety of nonstate groups and individuals who comprise the economy and society and who are not under direct state control but are possibly under its informal direction. Conceptually, the difference between formal state "control" and informal "direction" is subtle but crucial: the former implies membership of the state; the latter, exclusion from the state. On this basis, the private sector encompasses some forms of proxy actors such as criminal syndicates or privately owned firms (e.g., Kaspersky Lab)[11] that have

[9] Author interview with a senior official in the British Cabinet Office (February 17, 2017).
[10] "Chairman of the U.S. House Intelligence Committee Mike Rogers in Washington Post Live: Cybersecurity 2014," *Washington Post* (October 2, 2014).
[11] See Riley C. Matlack, M. Riley, and J. Robertson, "The Company Securing Your Internet Has Close Ties to Russian Spies," *Bloomberg* (March 15, 2015).

established informal working relationships with the government but it excludes state-affiliated civilian actors such as paramilitary militias (e.g., Estonian Cyber Defense League) or publicly controlled firms (e.g., Huawei).[12] The term "cyberweapon" or "arm" signifies the software and hardware instruments necessary to carry out cyber exploitation or attack. The term "active defense" – a contested and ambiguous notion – is broadly construed to denote the use of such instruments outside the defender's or other friendly terrain to prevent or preempt attack. This interpretation of active defense does not imply the use of any specific kind of cyberweapon; merely that the activity transpires in extra-defensive terrains (more on this below).

The paper has three sections: first, it defines the concept of active defense; second, it reviews the current state of private-sector active defense; and finally, it analyzes potential strategic benefits and risks associated with the development of private-sector arms.

The Meaning of Active Defense

The first step in analyzing private sector active defense is to define active defense. The notion features prominently in national strategy papers and public debates about cybersecurity, yet it has never been satisfactorily defined. Within official policy circles, there is no clear or precise definition; or if there is such a definition, it is veiled by government secrecy: the research community does not

[12] Huawei describes itself as an employee-owned "collective," but some commentators have questioned its freedom from Chinese state control. See Richard McGregor, *The Party: The Secret World of China's Communist Rulers* (New York: HarperCollins, 2010); and M. Rogers and C. A. D. Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE,* U.S. House of Representatives 112th Congress, Permanent Select Committee on Intelligence (October 8, 2012).

know its full contents. Official U.S. strategy papers supply only ambiguous meanings.[13] The Department of Defense describes "active cyber defense" as "[the] synchronized, real-time capability to deter, detect, analyze, and mitigate threats and vulnerabilities" – but reveals very little about the types of action involved. Other nations have publicly claimed possession of a capability but fail to define it even vaguely.[14] This section attempts to define active defense so that it may serve as a useful tool of analysis.

Three defining characteristics of active defense stand out: defensive purpose, out-of-perimeter location, and tactical flexibility. These characteristics may apply to the concept of active defense in any domain of conflict; the focus here will be on the cyber context.

Defensive Purpose

As the label implies, the aim of active defense is to enhance the security of the defender's assets: to deny proactively but not to penalize the attacker. The attacker, by definition, is affected only if he engages or prepares to engage or is perceived to engage the target. Thus the essence of active defense lies in the eye of the defender. It entails the reasonable *perception* – not necessarily the fact – of an adversary's intention and capability to attack. For this reason, retaliation to deter future attack does not qualify as active defense unless it seeks to degrade the attack sequence itself and transpires while the threat is still active.

Offensive activity that extends beyond the minimum threshold of action

[13] See *Department of Defense Strategy for Operating in Cyberspace* (Washington, D.C.: U.S. Department of Defense, July 2011), p. 7.
[14] See *Cyber Security Strategy, 2014–2017* (Tallinn: Ministry of Economic Affairs and Communications, 2014).

necessary to neutralize an imminent threat or endures after the threat has subsided also does not constitute active defense. Here the criterion of imminence is debatable: Does it include only tactical or also broader strategic threats? History provides a clue. As early as 1936, Japan presented a strategic threat to the United States by virtue of its intrinsic military potential and imperial designs in the Pacific, but it had few means to affect American interests directly. The Japanese threat did not become imminent until the Combined Imperial Fleet devised, in 1941, a viable tactical plan to attack Pearl Harbor. Thus the criterion of imminence demands the presence or the perception of a deployable, or nearly deployable, tactical capability to attack the defender.

What does imminence mean in the cyber domain? Two possibilities occur almost at once. The first and clearest scenario concerns the discovery within the defender's systems of sleeper malware – code customized to impair the target's functions but which has not yet struck. Of course, it may be difficult to ascertain the precise nature of the payload: Is it exploitative or destructive? But forensic testing may provide credible clues. A second scenario involves the detection of exploitative code whose aim the defender believes is to open a vector of access to attack or to harvest systems data that are relevant to the preparation of an attack. Whether the defender can infer from the activity an actual capability to disrupt the compromised system may depend on the activity's duration. The longer the length of action, the higher the chances the intruder will have harvested enough information to customize an attack payload. Here it may be difficult to ascertain the true intent of intelligence collection: Is it a case of stand-alone exploitation or a step in preparation for attack? The defender cannot penetrate the mind of the intruder. He may not even know the intruder's identity or location. Thus the

perception of imminence will rest – inevitably – on the reliability of the defender's forensic knowledge of the intrusion and on the soundness of the reasoning upon which he construes the intruder's intent, both of which will remain open to interpretation.

Out-of-Perimeter Location

The "active" quality of the concept refers not to offensive activity, as some thinkers suppose (see below), but to the activity's out-of-perimeter location. Passive measures are those the defender conducts within his own terrain; active measures are those he conducts *outside* it – that is, within adversarial or neutral terrain, including the terrain of innocent parties whose computer identity or functions the attacker has usurped. This characteristic of active defense features more prominently in British than in U.S. strategy papers, which do not clearly recognize it. For example, a report by the Joint Intelligence and Security Committee of Britain's House of Commons defines active defense as "interfering with the systems of those trying to hack into UK networks."[15]

The definition, it is important to realize, differs from the view of some information security professionals. One technical report described active defense as "the process of analysts monitoring for, responding to, learning from, and applying their knowledge to threats *internal to the network*." This definition, therefore, expressly excludes hacking back: "It is important to add the ending piece of 'internal to the network' to further discourage misrepresentation of the definition into the idea of a hack-back strategy. Analysts that can fall into this

[15] C. Green, "UK Becomes First Country to Disclose Plans for Cyber Attack Capability," *Information Age* (September 30, 2013).

category include incident responders, malware reverse engineers, threat analysts, network security monitoring analysts, and other security personnel who utilize their environment to hunt for the adversary and respond to them."[16]

Any proactive measures such as honeypots or sinkholes that exist entirely within servers that the defender legitimately controls do not qualify as active defense.[17] For if they did, why the controversy over expanding private sector arms? Law and custom broadly recognize the right of a computer operator to take whatever measures within his own terrain are necessary to defend it.

Tactical Flexibility

There is one sense in which common ambiguities in the meaning of active defense are warranted: the concept implies nothing about the scale, type, or intensity of the defender's action. Tactically, active defense may involve a variety of actions – intelligence collection, disruption (including destruction), or some combination of the two. On this basis, it is possible to conceive of three broad sorts of active defense: *nondisruptive*, *disruptive*, or *mixed* (in other words similar to a "multistage" cyberattack that involves both preliminary exploitation and subsequent disruption).[18] It is therefore imprecise to define active defense simply as offensive action to defeat an ongoing attack, although some observers

[16] Robert M. Lee, *The Sliding Scale of Cyber Security – A SANS Analyst Whitepaper* (Boston, MA: SANS Institute, 2015), pp. 9–11.
[17] Honeypots consist of decoy data that the defender uses to lure an attacker to study and disrupt his methods. See Loras R. Even, *Honey Pot Systems Explained* (Boston, MA: SANS Institute, July 12, 2000). Sinkholes refer to a DNS computer server that produces false data to prevent the attacker from using the true domain name. See Guy Bruneau, *DNS Sinkhole* (Boston, MA: SANS Institute, August 7, 2010).
[18] See David D. Clark and Susan Landau, "Untangling Attribution," *Harvard National Security Journal* (March 2011).

suggest this interpretation,[19] because the concept could, in fact, involve entirely nondisruptive measures, such as the insertion of exploitative beacons in enemy networks to capture threat data.

In sum, the chief distinguishing features of active defense are not the scale, intensity, or form of activity but rather *defensive* measures of threat neutralization – whether nondisruptive or disruptive or both – that defender implements *outside* his own or other friendly terrain. Table 1 summarizes and illustrates the differences between passive and active defense.

[INSERT TABLE 1 HERE]

The Current State of Affairs

The current state of private sector active defense may be assessed from four viewpoints: law, policy, practice, and capability. First is the legal viewpoint. In the U.S. federal context, the most important law is the Computer Fraud and Abuse Act (CFAA). Of the CFAA's seven sections, two are directly relevant to the regulation of active defense: section (a)(2)(C), which forbids unauthorized access to a computer to obtain data in it; and section (a)(5), which forbids the intentional use of computer code to impair the operations of a protected

[19] See, for instance, Alexander Klimburg and Jason Healey, "Strategic Goals and Stakeholders," in Alexander Klimburg, ed., *National Cyber Security Framework and Manual* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012), pp. 74–5 and 80; Tim Maurer and Robert Morgus, *Compilation of Existing Cybersecurity and Information Security Related Definitions* (New America, October 2012), p. 71; and Jay P. Kesan and Carol M. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace," *Harvard Journal of Law and Technology*, Vol. 25, No. 2 (Spring 2012), p. 460.

computer system.[20] Moreover, the Federal Wiretap Act's section 2511(2)(a)(i) forbids the unauthorized interception or recording of electronic communication transiting between machines. The fines for infringement of these rules can be severe.

The legal consequences of the recently passed Cybersecurity Information Sharing Act for private sector active defense in the United States are unclear. Possibly the bill will broaden the monitoring powers of private actors, but only if they work in conjunction with government authorities – in other words, as an informal arm of the state. Probably the changes will not be drastic. Although the bill allows the deployment of "countermeasures" that legitimately target threats and which damage data or machines on other networks, legally such countermeasures must be deployed within the defender's own network. Any resulting damage to external parties must therefore be unintentional.[21] Thus CISA's provision for countermeasures does not satisfy the out-of-perimeter criterion of active defense; it is beyond the scope of the present analysis.

There is little case law that elucidates the legal ramifications associated with the use of private sector arms.[22] Yet the prevailing legal viewpoint is clear: the practice of active defense is unlawful – if only because of the activity's second defining characteristic, that is, the intentional intrusion into or disruption of computers to which the defender lacks authorized access. Some officials have

[20] There are debates about the requirements of "authorization." See *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, third edition (Washington, D.C.: Department of Justice Office of Legal Council, 2009).
[21] It is unclear, however, whether intentional damage resulting from actions taken entirely within one's networks is lawful. See "Cyber-Surveillance Bill to Move Forward, Secretly" (Washington, D.C.: Center for Democracy and Technology, March 4, 2015).
[22] One notable case is Susan Clements Jeffrey vs. Absolute Software involving a company that used beacon technology to capture explicit data from a computer the operator did not know was stolen. The court ruled against the company. See "Absolute Software Settles Lawsuit Over Nude Photos," *Forbes* (September 6, 2011).

vocally pressed for changes in U.S. federal law that would allow the greater use of private active defense.[23] For now, however, the legal environment remains unequivocally proscriptive.

A second viewpoint concerns policy: official opinion reflects and supports the prevailing legal condition. The U.S. Department of Justice actively discourages exploitative active defense. One of its guidebooks states:

> A victimized organization should not attempt to access, damage, or impair another system that may appear to be involved in the intrusion or attack. Regardless of motive, doing so is likely illegal under U.S. and some foreign laws, and could result in civil and/or criminal liability. Furthermore, many intrusions and attacks are launched from compromised systems. Consequently, "hacking back" can damage or impair another innocent victim's system rather than the intruder's.[24]

Similarly, in a speech in 2015 the Assistant Attorney General, Leslie R. Caldwell, publicly denounced the use of strikeback techniques of any kind by firms and other private actors.

Other officials have occupied a more ambiguous position on the borderline between passive dissuasion and tacit acceptance. A recent comment by Admiral Mike Rogers, Director of the National Security Agency (NSA), embodies such

[23] See remarks by the Homeland Security Secretary, Janet Napolitano, in Joseph Menn, "Hacked Companies Fight Back with Controversial Steps," *Reuters* (June 18, 2012); and remarks by Chairman of the U.S. House Intelligence Committee Mike Rogers in "Washington Post Live: Cybersecurity 2014," *Washington Post* (October 2, 2014).
[24] *Best Practices for Victim Response and Reporting of Cyber Incidents* (Washington, D.C.: Department of Justice, April 2015).

ambiguity: "I'm not a big fan of the corporate world taking on this idea," he stated, but added: "It's not without precedence. If you go back to a time where nation states lacked capacity on their own, oftentimes they have turned to the corporate sector."[25] More revealingly, John Lynch, the head of the Justice Department's Computer Crime and Intellectual Property Section, drew a distinction between different types of active defense and their varying tolerability. He endorsed the nondisruptive use of beacon technology as lawful but condemned disruptive instruments, for example, artifacts that gain root access to modify other machines.[26] Moreover, the FBI has shown selective toleration of some uses of strikeback when it appeared urgent and proportionate to the security needs of the victim. Insofar as U.S. authorities are lenient toward private actors who employ defensive arms, they allow it not by changing the law but by evading it.

Third is practice: the question of what is actually happening regardless of the legal and policy conditions. The question is not easy to answer. Companies are no more translucent than governments when it comes to disclosing information about maneuvers within networks that they do not own or operate. The legal and reputational ramifications of disclosure are potentially high; they are not conducive to a culture of transparency on hacking and striking back. The near total absence of relevant case law reflects the prevailing culture of secrecy.

But if officials with knowledge of undisclosed cases are correct, the practice of active defense by the private sector far exceeds the record of it. As Tom Kellermann, a former member of the Commission on Cyber Security for the 44th

[25] Michael S. Rogers, "Cyber Threats and Next-Generation Cyber Operations," Keynote Speech at the Annual Cybersecurity Technology Summit, AFCEA, Washington, D.C. (April 2, 2015).
[26] Interview with John Lynch, Steptoe Cyberlaw Podcast (January 21, 2016).

Presidency, attested: "[Private] active defense is happening. It's not mainstream. It's very selective."[27] Of respondents to a 2012 poll at the Black Hat USA security conference, 36 percent claimed to have engaged in "retaliatory" hacking at least once (the poll was based on a sample of 181 conference attendees). Some American firms have recruited companies abroad to attack hackers on their behalf. At least a few times the freelancers provided strikeback as a courtesy to the victim. In brief, active defense activity by the private sector is increasingly common, if restrained, because of the moderate leniency of policymakers toward it.

Fourth, there is the question of capability: What is currently possible in the realm of private sector active defense and what future developments await? Again, a wall of secrecy conceals many facts. Like governments, firms and other private actors rarely disclose information about their capacity to operate antagonistically in external networks. Nonetheless, observable cases of strikeback reveal that private sector arsenals are significant and growing.

Some technology firms conduct advanced research on and guardedly deploy active defense capabilities. For example, some have deployed "spam-back" software (albeit without much success).[28] Microsoft possesses sophisticated measures to take down botnet command-and-control servers throughout the globe. In 2010, the company collaborated with the FBI to design and direct a remote "kill signal" to incapacitate machines infected with the Coreflood Trojan.[29] In 2014, Dell SecureWorks and Crowdstrike provided essential technical assistance

[27] Hannah Kuchler, "Cyber Insecurity: Hacking Back," *The Financial Times* (July 27, 2015).
[28] See Tom Spring, "Spam Slayer: Bringing Spammers to Their Knees," *PCWorld* (July 18, 2008).
[29] See Kim Zetter, "FBI vs. Coreflood Botnet: Round 1 Goes to the Feds," *Wired* (April 11, 2011).

to the FBI in an operation to take down the "GameOver Zeus"botnet.[30] Juniper Networks has begun to integrate elements of strikeback into its products.

Whatever the state of the private sector's active defense capability, actors, particularly large technology firms, are caught in an inconsistency between the legal and policy conditions – which are broadly but not entirely prohibitive – and the state of practice – which seems far more indulgent. A remark by Juniper Network's chief technology officer captures the discrepancy: "The dirty little secret is if there were no worries ethically and legally, everyone [would want] a 'nuke from orbit' button."[31]

Arming of the Private Sector: Strategic Benefits and Risks

Would private sector active defense impact national and international security positively or negatively? In examining these consequences, the discussion will consider effects on the defending players, their parent governments, innocent third parties, and international conflict stability.

Possible Benefits

The development of private sector arms may yield at least four positive consequences: improvement of strategic depth; closer civil–military integration; new options for plausible deniability by states; and a reduced defensive burden.[32]

One advantage involves *strategic depth*. Ordinarily, strategic depth in the

[30] See Brian Krebs, " 'Operation Tovar' Targets 'Gameover' ZeuS Botnet, CryptoLocker Scourge," *KrebsonSecurity* (June 2, 2014).
[31] Kuchler, "Cyber Insecurity."
[32] These consequences are positive from the perspective of private defenders and their parent governments; other players may not share this view.

cyber domain in the absence of active defense is very poor. The defender must wait until the attacker has made his move, after which the time to mount an effective defense is extremely short because the threat travels between machines at the speed of electrons and can achieve tactical results within a matter of seconds or even milliseconds. By contrast, the defensive response, unless it is automated, may require cumbersome procedures such as information-sharing and coordination with law-enforcement agencies, which in turn must take time to evaluate the legal, ethical, and tactical appropriateness of different policy options. For instance, it took the U.S. government several weeks simply to identify North Korea as the source of the attack against Sony Pictures in December 2014.[33] Moreover, detection itself may be very difficult to achieve. According to a report by Verizon, private firms take an average of 240 days to spot network intrusions.[34] The civilian sector owns or operates approximately 80–90 percent of critical computer systems and networks. Of U.S. government communications, including classified information, 98 percent travel over these networks.[35] It is therefore reasonable to assume that at all times some form of attack code resides undiscovered within much of the civilian sector's essential computer infrastructures.

One possible solution to the problem of strategic depth is greater

[33] The attackers activated the "Wiper" malware on 24 November; the FBI publicly attributed the attack to North Korea on 19 December. See "Update on Sony Investigation," Federal Bureau of Investigation (December 19, 2014), https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

[34] See 2016 Data Breach Investigations Report, Verizon (April 24, 2016), pp. 10–11. This figure is a simplification. The lag time between compromise and detection depends on the class and effects of the hostile action. A higher figure applies to cyber exploitation rather than cyberattacks. Indeed, some attacks – such as ransomware, which incapacitates the target machine – may be discovered immediately. The policy process from the time that investigators identified North Korea as the culprit to publicly outing it took longer than the time between when investigators first learned of the breach and when they identified North Korea.

[35] See Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (Oxford: Oxford University Press, 2014).

information-sharing between the private and public sectors. The Cybersecurity Information Sharing Act (CISA) aims to foster such sharing.[36] So far, however, firms have been reluctant to share, on a regular basis, their incident and threat data with the government. Much less are they willing to allow governments to monitor their networks directly owing to concerns about the privacy of proprietary information, the disclosure of which may harm corporate and client interests.

Private sector active defense could improve civilian strategic depth in a way that circumvents these concerns. It enables firms to identify and neutralize threats outside their networks without placing proprietary data at risk of government scrutiny. The insertion of beacons or "web bugs" – a form of exploitative active defense that some companies already use to track down stolen data – into adversary networks could enable these firms to design *disruptive* techniques that they can then use to neutralize threats at the point of origin, or, if the threat is in transit, in neutral systems. Here neutralization could be tactical, in other words a specific attack sequence is defeated but the attacker retains the ability to redeploy, or it could be strategic, in other words the attacker is dissuaded from or deprived of the ability to attack the target again. Exploitative tools could also support the government's *own* threat-monitoring and neutralization effort without themselves engaging in disruptive action. For example, third-party threat-intelligence companies may sell their services to the government, thereby serving as intermediaries between the victim and the government – an arrangement that could help to preserve the victim's anonymity.

[36] To share information derived from classified sources the U.S. government resorts to four selective commercial service providers: AT&T, CenturyLink, Lockheed Martin, and Verizon. See Andy Ozment, *DHS's Enhanced Cybersecurity Services Program Unveils New "Netflow" Service Offering* (Washington, S.C.: U.S. Department of Homeland Security, January 26, 2016), https://www.dhs.gov/blog/2016/01/26/dhs%E2%80%99s-enhancedcybersecurity-services-program-unveils-new%E2%80%9Cnetflow%E2%80%9D-service-offering.

A second advantage is enhanced c*ivil–military integration*. Western societies face an acute shortage of workers trained in technical disciplines relevant to cybersecurity, such as computer science and software engineering. The relevant skills base resides primarily in the private sector. Large technology firms (for example, Google, Apple, Microsoft) are able to offer salaries many times larger than military and security agencies (USCYBERCOM, NSA, GCHQ) can offer. "We are competing in a tough marketplace against a private sector that is in a position to offer a lot more money," lamented the U.S. Secretary of Homeland Security, Jeh Johnson. "We need more cybertalent without a doubt in D.H.S., in the federal government, and we are not where we should be right now, that is without a doubt."[37] Similarly, in Britain, the government skills gap is so severe that former GCHQ Director Iain Lobban said that his agency might have to employ non-nationals for a brief period – that is, before they, too, are inevitably absorbed by the private sector.[38] Another drain on skills occurs when defense contractors hire the manpower of government agencies, only later to sell their services back to the government.

Governments have reacted to asymmetry in the technological skills base in two ways: first, by attempting to assimilate civilian talent into loose state structures such as military reserves; and second, by cooperating with private technology providers to develop joint capabilities.

In the first approach, the government assumes a direct role in equipping the private sector. It drafts, trains, arms, and retrains elements of the civilian population in the methods of cyber operations. This may be achieved by

[37] Ron Nixon, "Homeland Security Dept. Struggles to Hire Staff to Combat Cyberattacks," *International New York Times* (April 6, 2016).
[38] See Oliver Wright, "GCHQ's 'Spook First' Programme to Train Britain's Most Talented Tech Entrepreneurs," *The Independent* (January 1, 2015); and Jamie Collier, "Proxy Actors in the Cyber Domain" (unpublished paper).

establishing a voluntary paramilitary defense force, such as Estonia's Cyber Defense League (*Küberkaitseliit*), a civilian defense organization that supports the military and Ministry of Defense;[39] or by way of conscription, as in Israel's Unit 8200, whose ranks include drafted servicemen who after an initial term of service enter the army reserves.[40] This approach has achieved moderate success in small nations such as Estonia and Israel, which have vibrant technological innovation hubs and a popular tradition of mass conscription. But it has paid only limited returns in large countries such as the United States and Britain where the National Guard or Reserves and the Territorial Army often fail to attract high-skilled elements of the civilian workforce.[41]

The second approach entails an extension of the concept of "private military companies" (PMCs) into the new domains. PMCs provide military and security services – even armed force – to the state or to other private entities.[42] This approach may be better suited to large nations with sizeable private technology industries but poorly developed traditions of military service. It would, however, require a greater commitment on behalf of participating companies to develop the sorts of strategic and tactical technologies that governments need to achieve national security goals. Some firms already provide the U.S. and other governments with sophisticated surveillance tools such as

[39] See Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm, "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," in M. Warren, ed., *Case Studies in Information Warfare and Security* (Reading: Academic Conferences and Publishing International Limited, 2013).
[40] See Lior Tabansky and Itzhak Ben Israel, *Striking with Bits? The IDF and Cyber-Warfare* (Cham: Springer, 2015).
[41] See "National Guard to Stand Up 13 New Cyber Units in 23 States," *Army Times* (December 15, 2015).
[42] See James Pattison, *The Morality of Private War: The Challenge of Private Military Companies and Security Companies* (Oxford: Oxford University Press, 2014); and A. Alexandra, D.-P. Baker, and M. Caparini, eds., *Private Military Companies: Ethics, Policies and Civil-Military Relations* (London: Routledge, 2008).

tracking and eavesdropping software.[43] Few companies, however, have invested in the other side of active defense – advanced disruptive tools – because of the legal and policy prohibitions or because the business case for doing so is not clear. Yet the private sector is well poised to develop them. Cisco's dominance of the router market, Google's near monopoly of online searches, and Microsoft's preponderance in the sale of desktop operating systems afford these firms tremendous (and legal) access to a significant proportion of Internet traffic and global hardware components. Some of this access is directly relevant to the harvesting of zero-day vulnerabilities and to the design of access vectors and payloads that governments require to mount sophisticated cyber operations.[44] CISA's relaxation of prohibitions against private sector exploitation performed under government sanction may foster more cooperation of this sort, although at present the structural incentives for such cooperation are not clear.

In brief, some elements of the technological sector possess merely by their existence a latent capacity to acquire sophisticated cyberweapons. The development of private sector cyber arms under informal government direction could enable governments to harness the civilian sector's technological prowess while avoiding the cumbersome organizational costs of traditional military formations.

Many firms, especially those with global commercial enterprises, may find the reputational costs of collaboration with government unacceptable, especially in a post-Edward Snowden world. Indeed, Google, Facebook, and other U.S. technology companies have sought to distance themselves from the perception

[43] See Sari Horwitz, Shyamantha Asokan, and Julie Tate, "Trade in Surveillance Technology Raises Worries," *Washington Post* (December 1, 2011).
[44] See Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data* (Santa Monica, CA: RAND, March 14, 2014).

that they work with the government to develop joint surveillance capabilities. But the alleged cooperation of RSA and Microsoft with the government proves that at least some level of complicity is acceptable even to large multinational firms with significant commercial interests abroad.[45] Most likely to succeed is the Israeli model of integrating the private sector into the national cyber establishment, which relies on the cultivation of ties with small start-ups that operate mostly in domestic markets – for example, NSO Group and Kaymera, which develop exploitative tools that allow the remote manipulation of smartphones.[46]

A third advantage is *plausible deniability*. Credible attribution of the source of a cyberattack is important because it enables the defender to inflict penalties on the attacker; without it the attacker can avoid them. States that develop offensive capabilities, therefore, have an incentive to devise means to complicate attribution (unless they desire positive attribution because they want to achieve a deterrent or demonstration effect). The more sophisticated the offensive operation, the smaller the universe of possible assailants – hence the higher the chances, *a priori*, that the defender will credibly attribute the attack so long as he detects it. This is a problem for the small number of states that possess the most advanced offensive weapons. After the Stuxnet attack became known, few people in Tehran asked: Did Jordan or Turkey do it? Similarly, no one asked: Was it Siemens (which built the Natanz nuclear facility's industrial control system) or Microsoft (the engineering stations)? Rather, the suspicion fell immediately upon the United States and Israel. Allowing the private sector to

[45] See James Vincent, "Edward Snowden Claims Microsoft Collaborated with NSA and FBI to Allow Access to User Data," *The Independent* (July 12, 2013).
[46] See Gabrielle Coppola, "Israeli Entrepreneurs Play Both Sides of the Cyber Wars," *Bloomberg* (September 29, 2014).

arm itself with sophisticated exploitative and disruptive tools would widen the field of theoretical attackers, thus complicating – in principle – the defender's attribution of the real attacker (a positive outcome for the attacker).

But the effect on attribution will be limited unless the firms in question are known to have offensive motives that seem credible to the adversary. Moreover, the development of PMCs may weaken the perception in the minds of adversaries of a neat separation between the public and private sectors. There is also the problem of "state responsibility," the principle of international law which stipulates that governments are responsible for harmful actions emanating from inside their jurisdictions. Thus the victim may attribute blame to the attacker's parent government even in the absence of direct government complicity. Fourth, is the reduction of the *defender's burden.* When a multinational firm is attacked, its possession of active defense capabilities could release the countries that host its headquarters or subsidiary branches from the burden of conducting defensive or retaliatory action against the offender. The transnational quality of modern production chains and commercial activity means that in contemporary society no large firm can enjoy the protection of a single state in all sectors of the global market within which it operates.[47] Firms may face attacks against interests and servers located in any one or in a variety of foreign jurisdictions. For example, considering the cyberattacks against Sony Pictures, a U.S.-based entertainment subsidiary of Sony, the Japanese technology conglomerate, the question is: In the absence of private sector arms, who strikes back – Washington or Tokyo? By enabling the company to respond itself, private sector

[47] See Stephen Krasner, "State Power and the Structure of International Trade," *World Politics*, Vol. 28, No. 3 (April 1976), pp. 317–47; and Richard N. Rosecrance, *The Resurgence of the West: How a Transatlantic Union Can Prevent War and Restore the United States and Europe* (New Haven, CT: Yale University Press, 2013).

arms would release the governments involved in the defensive response, assuming they desire one, from the burden of taking direct action.

The prospect of armed multinational enterprises acting under informal single-state direction recalls the partial successes of pirate merchants during the sixteenth and seventeenth centuries. Formally, pirates were unaffiliated (and thus differed from privateers, who operated under official government sanction). Yet occasionally they performed tasks at the direction of states, often changing flags in the process.[48] The use of pirates provided states with a means of waging undeclared and plausibly deniable war against other states.[49] Yet now, as then, the main obstacle to the success of the "piracy" model of public–private collaboration is the difficulty of aligning the goals of the state, which are generally political, with those of private firms, which are mainly economic.

Possible Risks

The use of cyber arms by the private sector entails at least three risks: foreign government penalties; innocent third-party harm; and inadvertent or accelerating international conflict. The last directly involves state interests and is potentially the gravest.

First is the danger of *foreign government penalties*. Even if CISA or other U.S. legislation permitted the private sector to deploy active defense tools, foreign domestic law will most likely continue to prohibit them; as explained above, almost all domestic penal codes presently criminalize active defense

[48] See Florian Egloff, "Cybersecurity and the Age of Privateering: A Historical Analogy," *Cyber Studies Working Paper No. 1*, University of Oxford (March 2015).
[49] See Fernand Braudel, *The Mediterranean and the Mediterranean World in the Age of Philip II* (Berkeley, CA: University of California Press, 1995).

measures. Thus, in such a world, the activity would be legal only in cases where the attack sequence originated in servers located exclusively within the defender's own jurisdiction and which did not cross any national boundaries – that is, in a negligibly small number of conceivable cyberattack scenarios.

It is possible that some other countries could amend their laws to allow the private sector the use of weapons in select cases. Or else governments may cast a blind eye when a player based in a friendly foreign country conducts active defense within its own jurisdiction under controlled conditions for demonstrably defensive aims. Two considerations would nevertheless diminish the appeal of private sector active defense. First, because they are on friendly diplomatic terms with the defender's parent country, the nations likeliest to permit or tolerate the use of private sector arms in their virtual terrain are also the likeliest to offer legal and police assistance during an attack implicating their jurisdiction – thus diminishing the need for private action in the first place. Second, and conversely, nations that have adversarial diplomatic relations with the defender's parent country are the least likely to permit or tolerate the use of private sector active defense against machines located within their jurisdiction. Even if they permitted the activity in some limited cases (for example, if the attacker is a common enemy), foreign nations would almost certainly penalize it in cases where they or their proxy agents were complicit in the attack. The difficulties of attaining certain attribution of the attack's sponsorship would mean that even if the defender believes the foreign government is not complicit, he may never be certain that this is in fact the case.[50] The possibility of punishment would remain

[50] Some thinkers question whether attribution is as hard as many observers believe it to be. See Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," *Journal of Cybersecurity*, Vol. 1, No. 1 (2015), pp. 53–67; and Thomas Rid, "Attributing Cyber Attacks," *Journal of Strategic Studies*

agonizingly real – especially if the inhibition to punish a firm by imposing financial penalties is lower than the inhibition to penalize another government with weightier measures such as economic sanctions.

A second risk is the potential for *innocent third-party harm*. Recall one of the main distinguishing aspects of active defense: it transpires outside the defender's terrain – including, possibly, in neutral terrain. Now note two important features of offensive cyber operations: they can be very difficult to attribute; and they often use multiple neutral machines and networks to access the target. Almost inevitably, therefore, active defense measures will impair to some degree the operations or data of third-party computer users, either because the defender misattributes the source of the attack to a machine that is in fact not involved because the attacker employs spoofing software that alters the compromise indicators (for example, the IP address); or because the defender correctly attributes the source or transit point of the attack but the identified machine is in fact innocent because the attacker has hijacked it. And as the number of injured parties multiplies, the potential for the conflict to accelerate and broaden grows.

The third type of danger is the gravest of all: *inadvertent and escalating conflict*, or the possibility of unwanted international crises. Some international relations thinkers have questioned the ability of private actors to destabilize the dynamics of interstate security competitions.[51] A world not far from the one in which we live challenges this view. Extending the private sector's ability to carry out active defense may produce instability in the following ways, *inter alia*:

(2015), p. 38.

[51] See Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015).

a) A private actor based in country A executes a disruptive active defense action on an attacking machine in country B. The government of country B interprets the action as an offensive strike by the government of country A. It retaliates against the defender and the government of country A.

b) A private actor based in country A executes a disruptive active defense action on an innocent machine in country C whose identity an attacker in country B has in fact spoofed. The government of country C retaliates against both the defender and the government of country A.

c) A private actor based in country A executes exploitative active defense activities against a machine in country B because he suspects that the machine may be preparing an attack. The machine in country B misinterprets the defender's move as a prelude to attack and launches its own preemptive strike against the defender in country A.

d) The governments of countries A and B are engaged in an international exchange of cyber blows that both sides seek to de-escalate and terminate. Armed private technology firms recruited into the conflict by the two countries misinterpret or choose to ignore their government's instructions. The firms continue to launch strikes against targets located in the other side's territory. The governments of countries A and B misinterpret the strikes as actions conducted or condoned by the opposing country. Rather than de-escalate, the conflict rapidly and uncontrollably intensifies.

e) An ideologically motivated and technically savvy employee of a private firm in country A illegitimately employs (in other words, for offensive

purposes) disruptive active defense tools against multiple innocent machines in country B while spoofing his identity to resemble a government player in country C (a hated country of the rogue employee). The government of country B misattributes the location of the attacker as country C. It attacks targets in country C. The government of country C retaliates in kind against targets in country B. The rogue employee repeats the deceptive maneuver but instead of attacking machines in country B targets those in country

f) The cycle repeats.

Convergence at the Cost of Collision

Equipment of the private sector with cyberweapons would intensify a broader trend in the contemporary era: the partial fusion of the world of states and the world of citizens and other groups. Many thinkers traditionally treat these two worlds as separate behavioral universes; they customarily ban private agents from theoretical models of the states system. Legal scholars point to the prevailing positivist doctrine by which the consent of states, whether formal or customary, is the only true source of international law.[52] Political scientists normally emphasize the state's supreme political authority in the ordering of both domestic and international affairs. Yet the growing influence of a variety of nonstate actors in the twenty-first century challenges these rigid models of political order. Multinational firms influence, sometimes decisively, the fiscal and

[52] Legal scholars who support the "natural law" tradition developed by Aquinas, Locke, and Vattel have challenged the positivist doctrine's position as the legitimate source of international law. See James L. Brierly, *The Basis of Obligations in International Law* (Oxford: Clarendon Press, 1958); and Hersch Lauterpacht, *International Law and Human Rights* (London: Stevens and Sons, 1950).

developmental agendas of states. Religious militant groups export pernicious ideologies and fighters to distant societies. Private military corporations affect the outcomes of foreign military occupations. Pirates scour the high seas and penetrate foreign coastlines. And so on.

The expansion of active defense activities to the private sector would intensify this flight of power away from the state. It would further challenge prevailing patterns of security competition and order in the international system. This disruptive trend could positively affect national security by improving strategic depth in a framework of interaction where private players are especially disadvantaged in defense; by fostering civil–military integration in a domain where technological prowess is indispensable but scarce; by offering governments new options to deny responsibility for offensive actions; and by lessening the sovereign burden of governments in a domain where the protection of the private sector – their traditional duty – is increasingly difficult to guarantee. That is, it may generate new opportunities for convergence, or cooperation between states and nonstate actors who share objectives and enemies.

The trend also invites new perils, however. A world in which private firms and citizen groups are free to carry out the prerogatives of national security policy against each other and against states is a world in which the risks of harm to innocent parties and accelerating conflict are potentially grave. The international system is the product of centuries of evolution in the design of mechanisms to regulate and restrain conflict among the main units: states. Continued erosion of that model through the empowerment of players which are alien to the system and that may not share the goal or even comprehend the intricate requirements of international order invites not only the benefits of deeper convergence but also

the dangers of collision between the fragile states system and the chaotic global system. Cyber civil defense should remain a reactive enterprise.

Table 1: Passive vs. active defense in the cyber domain

	Within Perimeter	**Out of Perimeter**
Undisruptive defense	**Passive** Resilience, redundancy, organizational reform, information sharing	**Active** Standalone defensive exploitation (e.g. to gain knowledge of the adversary's capabilities)
Disruptive defense	**Passive** Honeypots, sinkholes, beacon neutralization	**Active** Disruption of the adversary's command and control systems (may require preliminary exploitation)