The Heritage Foundation

BACKGROUNDER

No. 3188 | MAY 5, 2017

Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense

Paul Rosenzweig, Steven P. Bucci, PhD, and David Inserra

Abstract

The failure of the government to provide adequate protection has led many cybersecurity analysts, scholars, and policymakers to suggest that there is a need for private-sector self-help. If the government is unable or unwilling to take or threaten credible offensive actions to deter cyberattacks or to punish those who engage in them, it may be incumbent upon private-sector actors to take up an active defense. In other words, the private sector may wish to take actions that go beyond protective software, firewalls, and other passive screening methods—and instead actively deceive, identify, or retaliate against hackers to raise their costs for conducting cyberattacks. Taking into consideration U.S., foreign, and international law, the U.S. should expressly allow active defenses that annoy adversaries while allowing only certified actors to engage in attribution-level active defenses. More aggressive active defenses that could be considered counterattacks should be taken only by law enforcement or in close collaboration with them.

One of the most debated concepts in cybersecurity is active cyber defense. Cyber theft and espionage are rampant, costing governments and private-sector actors hundreds of billions of dollars in losses annually.[1] To a large degree, government efforts to reduce the risks of such cyber intrusions have proven ineffective—one need only think of the revelations of significant intrusions into more than 140 American companies by Chinese cyber hackers affiliated with the People's Liberation Army, as well as continued intrusions into both government systems (the Office of Personnel Management) and private networks (such as the Democratic National Committee, the Clinton presidential campaign, Target, or Sony).[2]

This paper, in its entirety, can be found at **http://report.heritage.org/bg3188**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Key Points

- If the government is unable or unwilling to deter cyberattacks or punish those who engage in them, it may be incumbent upon private-sector actors to take up an active defense.
- "Active cyber defense" goes beyond protective software, firewalls, and other screening methods—and actively deceives, identifies, or retaliates against hackers (known as "hack back") to raise their costs for conducting cyberattacks.
- Before the U.S. authorizes private hack back, it must consider not only U.S. laws, but also foreign and international laws governing cyberspace.
- Congress should move beyond the status quo and establish a new active cyber defense system that enables the private sector to identify and respond to hackers more effectively.
- This new policy must be limited to minimizing unintended effects and the risk of additional escalation, but it is an important step for U.S. cybersecurity.

The failure of the government to provide adequate protection has led many cybersecurity analysts, scholars, and policymakers to suggest that there is a need for private-sector self-help. The 2016 Republican platform even included a provision regarding active cyber defense.[3] If the government is unable or unwilling to take or threaten credible offensive actions to deter cyberattacks or to punish those who engage in them, it may be incumbent upon private-sector actors to take up an active defense. In other words, the private sector may wish to take actions that go beyond protective software, firewalls, and other passive screening methods and instead actively deceive, identify, or retaliate against hackers to raise their costs for conducting cyberattacks.

While these private-sector actions take many forms, they go by the collective name of "active cyber defense" and include actions that are commonly referred to as "hack back." In essence, it is the idea that private-sector actors may push back at the hackers who are attacking them. Before the United States authorizes such activities by private-sector actors, it is important to consider not only how to manage effects of these actions within U.S. domestic law, but also foreign and international law governing cyberspace and the implications of such laws for U.S. private actors that engage in active cyber defense.

This *Backgrounder* will examine what an appropriate active cyber defense regime could look like. There are multiple models and analogies of active defense that should provide clarity to policymakers regarding the bounds of acceptable private responses. Additionally, these models detail how active cyber defense regimes may or may not fit within the ambit of existing laws. Congress should move beyond the status quo and establish a new active cyber defense system that enables the private sector to attribute and respond to hackers more effectively. At the same time, this new policy must be carefully limited to minimize unintended effects and the risk of additional escalation. This constrained system of authorized active cyber defense would be an experiment that must be carefully monitored and adjusted, but it is an important step for U.S. cybersecurity.

A Spectrum of Active Cyber Defense

There is a spectrum of active cyber defense, much of which lies in a gray zone between clearly illegal and clearly legal. George Washington University's Center for Cyber and Homeland Security has created some helpful graphics that describe the techniques along this spectrum. (See Figure 1 and Figure 2.)

This spectrum can also be thought of as being divided into three types of responses: those that are (1) an annoyance, (2) an attribution, or (3) an attack.[4]

Annoyance. Techniques that serve as an annoyance to adversaries are the least aggressive and the most legally permissible form of active cyber defense. They go beyond passive defenses such as firewalls, passwords, and a properly configured network and yet are still composed of techniques that occur primarily or entirely on the defender's network. These techniques include information sharing, tar pits and honeypots, various denial-and-deception techniques, and intrusion-prevention or hunting systems. In essence, these techniques are akin to deterrence by denial—ideally, they make it difficult for a

1. McAfee estimates that yearly cyber losses are likely greater than $400 billion for the world economy. See "Net Losses: Estimating the Global Cost of Cybercrime, Economic Impact of Cybercrime II," McAfee and the Center for Strategic and International Studies, June 2014, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf (accessed November 3, 2016).
2. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, FireEye, Inc., undated, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (accessed January 13, 2017); Shane Harris, "Team Obama Knows China Is Behind the OPM Hack. Why Won't They Say So?" *The Daily Beast*, July 20, 2015, http://www.thedailybeast.com/articles/2015/07/20/team-obama-knows-china-is-behind-the-opm-hack-why-won-t-they-say-so.html (accessed January 18, 2017); news release, "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security," Office of the Director of National Intelligence, October 7, 2016, https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement (accessed January 18, 2017); and Bob Orr, "Why the U.S. Was Sure North Korea Hacked Sony," CBS News, January 19, 2015, http://www.cbsnews.com/news/why-the-u-s-government-was-sure-north-korea-hacked-sony/ (accessed January 18, 2017).
3. 2016 Republican National Convention, "Republican Platform 2016," July 2016, https://prod-static-ngop-pbl.s3.amazonaws.com/media/documents/DRAFT_12_FINAL[1]-ben_1468872234.pdf (accessed November 11, 2016).
4. John Strand, "How I Learned to Love Active Defense," *Dark Reading*, July 20, 2015, http://www.darkreading.com/attacks-breaches/how-i-learned-to-love-active-defense/a/d-id/1321361 (accessed November 15, 2016).

hacker to attack and exploit the defender's systems successfully, making the hacker give up.

Attribution. This set of techniques does not necessarily annoy a hacker, but instead seeks to identify him. While annoyance takes place primarily or entirely on the machine of the defender, attribution begins to reach further out to find files stolen by and the computers used by the hackers. As described in Figures 1 and 2, beaconing programs and intelligence gathering in the deep web or darknet would be considered attribution and intelligence-gathering activities. Because some of these methods require accessing an attacker's network, even without altering or modifying its content or behavior, attribution techniques are considered more aggressive and hence more legally problematic.

Attack. The final set of techniques involve attacking a hacker's systems and include botnet takedowns, white hat ransomware, efforts to recover stolen data by hacking back, or "hack back" operations designed to disrupt or destroy another system. Such actions are increasingly aggressive and seem to fall more within the province of law enforcement or the military than the private sector. At this level, if undertaken by the private sector without legal authorization, they are likely to fall afoul of domestic and foreign laws.

Domestic, Foreign, and International Cyber Laws

In the United States, scholars have been debating the legality of active cyber defenses, especially hack back. To date, much of that examination has focused on domestic American law.[5] This is an important conversation, because if the U.S. were to conclude as a matter of policy that it was appropriate to allow private-sector actors to conduct active cyber defense, the U.S. would have to consider which, if any, laws require changes.[6] No one wants to turn the Internet into a digital free-fire zone. Nor does the U.S. need everyone who goes online to see himself as a cyber vigilante. That said, given that the government does not appear to have sufficient capabilities to fight all of these battles and that many private-sector entities do have excellent and talented personnel on their staffs to do so, changes should be considered.

But American authorization of private-sector offensive action would hardly end the discussion. It would merely begin it. Cyberspace is, after all, an international trans-border domain. Cyberattacks and espionage against American companies often originate overseas and transit foreign servers. Thus, any American hack back would almost inevitably involve other countries and their laws. So consideration must be given to the question of whether private-sector hack back violates (or is authorized by) the domestic laws of other nations or any international conventions or customary international law.

An examination of how American, foreign, and international law affects American private-sector hack back reveals three fundamental conclusions:

1. Existing U.S. law hampers active cyber defense. Controlled and monitored authorities must be constructed to improve the deterrent effects of private-sector actions, since merely "taking off the gloves" could be self-defeating.

2. Hack back by an American private-sector actor will almost certainly violate the domestic law of the country where a non-U.S. computer or server is located.

3. To the extent that any customary international law exists at all, it is likely to discourage private-sector self-help outside the framework of state-authorized action.

Domestic Law. The debate regarding domestic law and the lawfulness of active cyber defenses revolves around the Computer Fraud and Abuse Act (CFAA) of 1986, which prohibits accessing "a protected computer without authorization." Given that active cyber defenses may probe, follow, or other-

5. See, for example, "The Hackback Debate," Steptoe Cyberblog, http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/ (accessed January 12, 2017).

6. See, for example, "Rep. Gohmert Wants a Law that Allows Victims to Destroy the Computers of People Who Hacked Them," TechDirt, March 19, 2013, https://www.techdirt.com/articles/20130316/01560522347/rep-gohmert-wants-law-that-allows-victims-to-destroy-computers-people-who-hacked-them.shtml (accessed January 12, 2017), and Steven P. Bucci, Paul Rosenzweig, and David Inserra, "A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation *Backgrounder* No. 2785, April 1, 2013, http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace.

wise interact with the attacker beyond the defender's computers, such actions may be considered unauthorized access in violation of the CFAA. The formal position of the U.S. government is that any activity by a defender on another individual's network is illegal and a criminal violation of the CFAA.

The Justice Department's manual on *Prosecuting Computer Crimes*[7] states that:

> Although it may be tempting to do so (especially if the attack is ongoing), the company should not take any offensive measures on its own, such as "hacking back" into the attacker's computer—even if such measures could in theory be characterized as "defensive." Doing so may be illegal, regardless of the motive. Further, as most attacks are launched from compromised systems of unwitting third parties, "hacking back" can damage the system of another innocent party.

Thus, while as an intellectual matter criminal liability under the CFAA is a hotly debated topic, there seems to be little doubt that most courts would hold a domestic hack-back actor criminally liable. So any legislation considering the issue of hack back or active cyber defense must deal with this statute.

Nor would the CFAA be the only American law applied. For example, many states have laws that expand on the Wiretap Act and also make it illegal to intercept communications without the consent of both parties—consent that the hacker will not give.[8] Any federal law authorizing active cyber defenses would therefore have to modify the CFAA and preempt contrary state law. Definitional precision in drafting this new language is essential so that the original purposes of those laws are achieved while allowing for tailored cybersecurity practices.

Foreign Cyber Laws and Their Implications. Wholly apart from strictly domestic American law, another topic that must be considered is how the laws of foreign nations will affect private-sector hack back. In almost all circumstances, American private actors who undertake cyber defensive measures against their opponents will wind up affecting

FIGURE 1

Spectrum of Active Cyber Defense

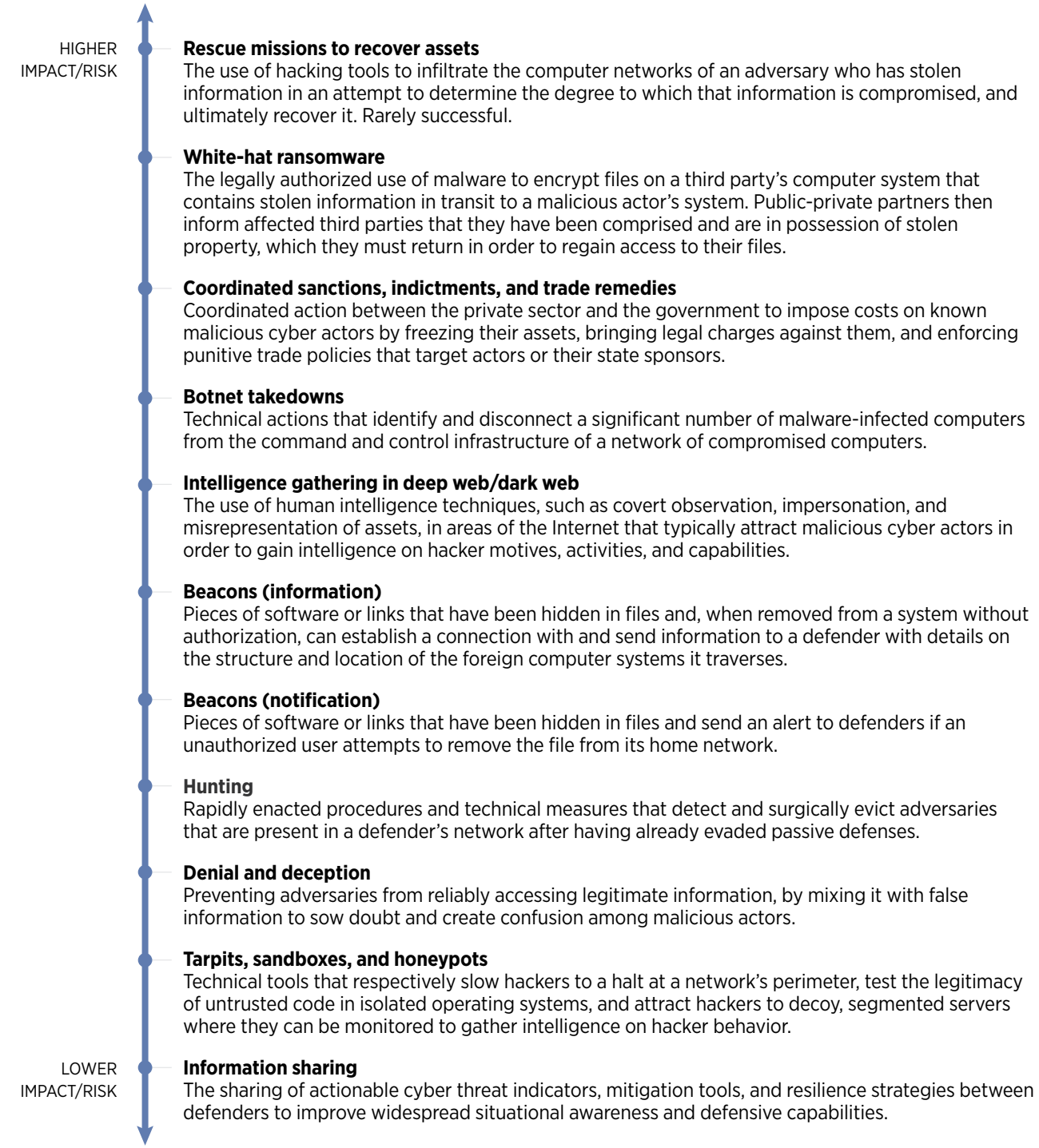
SOURCE: Center for Cyber and Homeland Security, The George Washington University, "Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats," October 2016, p. 10, Figure 2, https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf (accessed November 15, 2016).

BG3188 heritage.org

7. U.S. Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, *Prosecuting Computer Crimes*, January 14, 2015, p. 180, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (accessed January 12, 2017).
8. Christopher Jarko, "Finding the Fine Line—Taking an Active Defense Posture in Cyberspace Without Breaking the Law or Ruining an Enterprise's Reputation," SANS Institute, September 2014, https://www.sans.org/reading-room/whitepapers/legal/finding-fine-line-%E2%80%93-active-defense-posture-cyberspace-breaking-law-36807 (accessed November 23, 2016).

FIGURE 2

Active Defense Techniques Defined



SOURCE: Center for Cyber and Homeland Security, The George Washington University, "Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats," October 2016, p. 10, Figure 2, https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf (accessed November 15, 2016).

BG3188 ☎ heritage.org

computers located outside the borders of the United States. When this occurs, American actors may be subject to foreign cybersecurity laws. Before the U.S. government authorizes individual actors to engage in active cyber defense, and before U.S. companies engage in such actions, the U.S. should consider how actions taken by its private sector will be perceived in target or transit states where the effects of U.S.-based actions might be felt.

In surveying the laws of other nations, it becomes clear that other countries are quite skeptical of the concept of private-sector self-defense. To cite but one example, hack back is illegal in Germany, though several anecdotal reports suggest that German private entities use active cyber defensive techniques anyway.[9] The German prohibition, known as "The Hacker Paragraph," is Section 202a of the German Criminal Code and provides in relevant part: "Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorized access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years, or a fine."[10] Other provisions explicitly make phishing a crime and criminalize any acts in preparation for data espionage or phishing.[11] Germany is not alone in this regard.[12]

Since the prospect of non-American criminal prosecution is a realistic one, U.S. action on authorized private-sector defense must proceed cautiously. While criminal prosecution or the threat of it has been ineffective in deterring overseas hackers of American interests, it is precisely the foreign and unlawful nature of many of these actors that makes the threat of prosecution an empty one. Many hackers are beyond the reach of American law and reside in countries with which the U.S. has no effective extradition program for cyber offenses.

On the other hand, when a U.S. private actor's actions have collateral effects in an allied country, such as Germany or Japan, it is quite conceivable that American legal authorities would honor an appropriately couched request for mutual legal assistance or extradition from the affected nation. The prospect of criminal prosecution is therefore higher for American actors precisely because the U.S. government is a lawful actor on the world stage. Even for countries where extradition is not a realistic prospect (the U.S. will not and cannot, for example, extradite an American to stand trial in China for hack back), there will be other avenues of retaliation that must be considered. Most American private-sector actors who have the resources to contemplate self-defense, for example, will be corporations or individuals with a multinational presence. Even allowing for difficulties of attribution, it is quite likely that those overseas assets will be at risk if the American parent entity conducts private offensive operations.

Customary International Law or Treaties. Finally, to conclude the analysis of the international aspects of private-sector active cyber defenses, an important question must be answered: Is international law even relevant to the question of private-sector hack back? The most reasonable answer to this question is, quite simply, "no."

International law is not formally relevant for at least two independent and important reasons. First, a survey of existing international instruments shows that private-sector offensive cyber activity is nowhere mentioned. Thus, as a formal matter, current international law is completely silent on the topic. Second, and rather more fundamentally, with very limited exceptions,[13] international law is directed at nation-state actors and

9. Davi Ottenheimer, "Hack Back Is Here," Flyingpenguin, June 8, 2012, http://www.flyingpenguin.com/?p=17043 (accessed December 21, 2016).
10. German Criminal Code, § 202a, http://www.gesetze-im-internet.de/englisch_stgb/ (accessed November 15, 2016).
11. Ibid., §§ 202(b) and (c).
12. "Wetgeving bestrijding cybercrime," *Ministerie van Veiligheid en Justitie*, October 15, 2012, http://www.rijksoverheid.nl/ministeries/venj/documenten-en-publicaties/kamerstukken/2012/10/15/wetgeving-bestrijding-cybercrime.html (The Netherlands law; text in Dutch) (accessed November 15, 2016); Lucian Constantin, "Dutch Government Seeks to Let Law Enforcement Hack Foreign Computers," *PC World*, October 19, 2012, http://www.pcworld.idg.com.au/article/439620/dutch_government_seeks_let_law_enforcement_hack_foreign_computers/ (accessed November 15, 2016); and Rotem Pesso, "IDF in Cyberspace," Israel Defense Forces, March 6, 2012, http://www.idf.il/1283-16122-en/Dover.aspx (accessed November 15, 2016).
13. For example, the Rome Statute of the International Criminal Court (U.N. Doc. A/CONF.183/9), http://legal.un.org/icc/statute/99_corr/cstatute.htm (accessed January 13, 2017).

is intended to control their behavior.[14] Nations sign treaties and are, in turn, bound to act on the obligations they undertake. In general, international law has nothing specific to say about private actors and their behavior. As noted below, there may be some small exceptions to that in the context of customary international law regarding self-defense against piracy. In the main, however, formal international treaties have no apparent direct application to the questions being considered.

Analogies in the Physical World for Responding in Cyberspace

Cyberspace is a relatively new space for expression, communication, commerce, and conflict. Together with its inherent features, such as anonymity and lack of built-in security, understanding how to respond to aggression in cyberspace can be difficult. As a result, scholars and experts have turned to other areas of law and conflict for potential analogies that can be used to craft appropriate responses and rules. These analogies are not perfect, but they can inform the way policymakers think about active cyber defense and hack back and which role such methods should play in defending U.S. networks.

Privateers and Letters of Marque and Reprisal. On one end of the spectrum is the analogy of active cyber defense to letters of marque and reprisal.[15] A wartime tactic, letters of marque allowed privateers to seize the property of a foreign country on the high seas. Outlined in Article 1, Section 8 of the U.S. Constitution, Congress has the authority to issue letters of marque—a power last invoked during the War of 1812.[16] Letters of marque in cyberspace would involve techniques that are at the very aggressive "attack" end of the active cyber defense spectrum involving sanctioned attacks on hackers.

While this analogy has interested many individuals, providing letters of marque to U.S. companies is not a good model for future active cyber defense for at least three significant reasons:

1. Letters of marque are effective precisely because they motivate private actors through the profit motive. Privateers are allowed to sell a portion of what they seize for their own benefit. Cyber letters of marque could incentivize overly belligerent cyber aggression, with cyber privateers authorized to engage in widespread looting of presumed hackers' computers, potentially even taking destructive action against those systems.[17]

2. In effect, piracy and espionage that steal trade secrets, intellectual property, and other valuable information will be activity to the benefit of private companies that do not keep the strong U.S. commitment to property rights and a free and open network. While such actions might be appropriate in the context of an armed conflict, they are more problematic outside of a wartime situation.[18]

3. This analogy fails to address the myriad of foreign laws that are likely broken by such privateering. As noted above, active cyber defenses break foreign law—and the more aggressive the authorized

14. For example, Responsibility of States for Internationally Wrongful Acts (U.N. Doc. annex to General Assembly resolution 56/83 of 12 December 2001, and corrected by document A/56/49(Vol. I)/Corr.4)), 2001, http://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf (accessed January 13, 2017).
15. Jeremy A. Rabkin and Ariel Rabkin, "To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict," Hoover Institution, Koret-Taube Task Force on National Security and Law, *Emerging Threats Essay,* 2012, http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rabkin.pdf (accessed November 15, 2016), and Jeremy Rabkin and Ariel Rabkin, "Hacking Back Without Cracking Up," Hoover Institution Working Group on National Security, Technology, and Law, *Aegis Paper* No. 1606, June 28, 2016, http://www.hoover.org/sites/default/files/research/docs/rabkin_webreadypdf.pdf (accessed November 15, 2016).
16. *The Heritage Guide to the Constitution: Fully Revised Second Edition, ed. David F. Forte and Matthew Spalding* (Washington: The Heritage Foundation, 2014).
17. Ibid.
18. The White House, "United States Counter Piracy and Maritime Security Action Plan," June 2014, https://obamawhitehouse.archives.gov/sites/default/files/docs/united_states_counter_piracy_and_maritime_security_action_plan_2014.pdf (accessed February 2, 2017), and news release, "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference," The White House, September 25, 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint (accessed November 15, 2016).

activity, the less likely it is that the United States can gain international consensus around a norm approving such efforts.

Self-Defense and Piracy on the High Seas. While international law has little to say directly on the issue of cyber hacking, one potential analogy is the law of piracy. After all, some call cyberspace a highway of commerce—much as the ocean functions. Hackers stealing intellectual property are a nice analogy to pirates who steal physical property.

An important aspect of piracy law is the general right of self-defense. Recent international instruments that were intended to clarify existing rules in response to the upsurge in piracy off the coast of Somalia make it relatively clear that private entities may use violent force in self-defense to prevent crimes that threaten life. This analogy includes techniques that would be found in the attack end of the spectrum, but only to the extent that the cyber "piracy" is life-threatening. There is less agreement with respect to the converse principle: the use of nonviolent measures in self-defense when life is not threatened.

In November 2010, the International Code of Conduct for Private Security Service Providers (ICOC) was opened for signature. As of late 2013, more than 708 companies from 70 countries had signed,[19] though only 101 private companies had formally become members of the ICOC Association as of 2016. The ICOC requires security service providers to avoid the use of force if possible and, if required, to use only proportionate force in response. Violence (in the form of firearms) is prohibited except in case of imminent threat of death or serious injury or to prevent a "grave crime."[20]

American practice seems to have expanded on that rule to encompass a broader scope for self-defense. In 2009, the Coast Guard and the Department of Homeland Security (DHS) issued a Port Security Advisory titled "Guidance on Self-Defense and Defense of Others by U.S. Flagged Commercial Vessels Operating in High Risk Waters."[21] The guidance suggested, consistent with the codification in the ICOC, that lethal force in self-defense was strictly limited to circumstances where there was a danger of death or serious bodily injury. But the guidance then went further to make clear that the *non*-deadly use of force could be authorized by a vessel's master to protect the vessel or cargo from theft or damage. In 2010, Congress affirmed the importance of self-defense by providing additional liability protections for those who engage in self-defense in accordance with Coast Guard rules.[22] Taken as a model for cyber defenses, this would certainly offer some comfort to those who think that international law will authorize a limited right of self-defense.

This international version of a right of self-defense, however, is actually quite limited and is most likely restricted to areas of action involving a company's defense of its own networks. When an actor seeks to use active cyber defense measures, analogous to "hot pursuit" of pirates, the law of piracy suggests that only a state may act—not a private citizen.[23] In fact, that right may be even more limited. The right of hot pursuit ceases as soon as the ship being chased "enters the territorial sea of its own country or of a third State."[24] In other words, once the pirate ship enters home waters or leaves the open area of the high seas, the pursuing state must stop, and any attempt to continue the pursuit must rely on the authority of the nation where the pirates have taken refuge.

19. Graham Penrose, "International Code of Conduct for Private Security Service Providers," TMG Corporate Services, June 18, 2014, http://tmgcorporateservices.com/blog/2014/06/18/107-icocfpssp.html (accessed November 15, 2016).
20. International Code of Conduct for Private Security Service Providers, Arts. 30–32, https://icoca.ch/sites/all/themes/icoca/assets/icoc_english3.pdf (accessed January 13, 2017).
21. Port Security Advisory (3-09), "Guidance on Self-defense or Defense of Others by U.S. Flagged Commercial Vessels Operating in High Risk Waters," U.S. Department of Homeland Security, U.S. Coast Guard, International Port Security Program, June 18, 2009, http://www.marad.dot.gov/documents/Port_Security_Advisory_3-09_Self_Defense.pdf (accessed January 13, 2017).
22. Charlie Papavizas and H. Allen Black, "Coast Guard Finalizes U.S.-Flag Piracy Self-Defense Guidance," Winston & Strawn LLP, July 6, 2011, http://www.winston.com/en/maritime-fedwatch/coast-guard-finalizes-u-s-flag-piracy-self-defense-guidance.html (accessed November 15, 2016).
23. Convention on the High Seas, Art. 19, 1958, http://www.gc.noaa.gov/documents/8_1_1958_high_seas.pdf (accessed January 13, 2017), and United Nations Convention on the Law of the Sea, Art. 100, 1982, http://legal.un.org/diplomaticconferences/lawofthesea-1982/lawofthesea-1982.html (accessed January 13, 2017).
24. Convention on the High Seas, Art. 23(2).

So the analogy of self-defense aboard private vessels suggests that private actors can do little beyond their own networks and where hot pursuit might be allowed for nation states; it is limited by national borders. While it is comforting that the piracy analogy recognizes some authorized defensive acts, the scope of that authorization turns out to be quite limited and of little practical utility to an assessment of active cyber defenses.

Private Security. With this in mind, it appears that a better model is the private security business. As practiced today in the physical world, private security firms can obtain licenses to carry weapons, to detain trespassers, and even to use deadly force in specified situations to protect their own facilities and people or those of their clients. These organizations have to meet certain standards, often set by the state in which they operate.[25]

The same sort of process could be applied to active cyber defense. Separate security firms could be established (possibly within existing cybersecurity companies) that go through a process to be licensed. They would be expected to understand the limitations of their authorities and then be hired to act in this capacity for others, either on an as-needed basis or in an ongoing in-house capacity. A variation would be a highly competent tech company establishing a licensed organization within its own workforce to undertake the same function for itself. These security firms would be allowed to engage in active cyber defense that does not result in physical destruction or result in harm to innocent individuals or their systems. As with the prior analogies, this one allows techniques that do constitute attacks, but it suggests greater restraint and restrictions on what kinds of attacks are allowed.

Under this construct, only authorized teams would be legally permitted to engage in active cyber measures. In order to do so, they would need to demonstrate the ability to identify their adversary, the efficacy of their techniques, and an understanding of the legal boundaries of their activities. These limits would significantly ease the vigilante concern[26] that many have regarding hack back and would ensure a measure of order and control while relieving the government of the exclusive responsibility for actively defending private networks. An additional advantage would be that setting up such a system would better position the U.S. to defend its networks from an adversary with strong cyber capabilities in the event of a significant conflict.

While this analogy may seem more reasonable than letters of marque or self-defense on the high seas, the most significant challenge of such a system is foreign law. The cybersecurity guards in this analogy are not merely guarding a bank in the U.S., but will often be crossing borders to stop foreign hackers. As mentioned earlier, foreign laws outlaw and seek to punish those who hack into systems residing in other countries. If a U.S. company used an authorized private cybersecurity company, it might be breaking the law of the country in which the target systems reside. While there may be minimal risk of that country responding if the effects of the active cyber defenses are restrained or unnoticed, a hack back with significant collateral effects could prompt that country to pursue legal recourse against the U.S. company, harming its business and reputation.[27] In most cases, such risks will prevent businesses from engaging in active cyber defense and thus limit the applicability of this approach.

A properly limited security-guard model, however, could avoid some of the concerns regarding breaking foreign laws. For example, a potentially viable system of active cyber defense might generally forbid destructive hack back but allow limited use of white-hat ransomware as a trap that is activated when data are stolen and also permit participation in botnet takedowns that are coordinated with law enforcement.

It seems that the best way forward is to authorize private security protection inside a limited framework.[28] Most saliently, the U.S. should exclude

25. Andrews International Training Center, "Security Guard Licensing Requirements," http://www.ussecurityassociates.com/ai-training/statereq.html (accessed November 15, 2016).
26. Eduard Kovacs, "Hacking Back: Industry Reactions to Offensive Security Research," *Security Week*, November 13, 2015, http://www.securityweek.com/hacking-back-industry-reactions-offensive-security-research, and Sara Sorcher, "Influencers: Companies Should Not Be Allowed to Hack Back," *Christian Science Monitor*, April 1, 2015, http://www.csmonitor.com/World/Passcode/Passcode-Influencers/2015/0401/Influencers-Companies-should-not-be-allowed-to-hack-back (accessed January 13, 2017).
27. Sean L. Harrington, "Cyber Security Active Defense: Playing with Fire or Sound Risk Management?" *Richmond Journal of Law & Technology*, Vol. 20, No. 4 (2014), http://jolt.richmond.edu/v20i4/article12.pdf (accessed November 15, 2016).
28. Rabkin and Rabkin, "Hacking Back Without Cracking Up."

the most aggressive end of the response spectrum—private cyber guards should have no authority to "return fire." Instead, they might only be empowered to use cybersecurity tools that could be described as annoyance and attribution techniques. For example, a certified cyber private responder might be given legal protection from legal ambiguities surrounding various techniques of beaconing, which are akin to placing a tracking device within a set of files that can relay information when stolen. The CFAA and various state versions of the Wiretap Act, as mentioned earlier, are two sets of law that could be problematic for companies wishing to engage in beaconing.[29] Additionally, cyber responders could be given limited legal protection for aggressive counterintelligence activities, such as investigating hacker communities, that may require them to be in the presence of otherwise illegal material or activities such as child pornography.[30]

This limited formulation of cybersecurity guards is similar to existing cybersecurity services offered by a variety of companies in the U.S., including CrowdStrike, FireEye, Cylance, and many others. By providing such actors with additional limited authorities and protections, private companies will be able to provide enhanced cybersecurity services while also avoiding many of the domestic and foreign legal hazards that apply to attacks.

For this model to be most effective, however, close coordination with and action by government authorities is a requirement. Under this model, the private sector will gain new sources of actionable intelligence on hacks and hackers but still need law enforcement and prosecutors to use such intelligence to respond. When the private sector presents its intelligence and evidence gathered through these attribution methods, law enforcement must be willing to act. While not every piece of intelligence can be acted on or used in court, it is not unreasonable to expect the government to be more vigorous in its investigation and prosecution of cybercrime. Furthermore, while in cases of state-conducted or state-sponsored hacking there may be a government desire to protect intelligence sources and methods, the attribution in this system will have been privately developed. This privately acquired information may be released anyway, rendering the government's concern moot and permitting a more assertive stance by law enforcement against hackers.

Defending U.S. Cyber Systems Responsibly

Cyber self-defense can be a valuable tool for deterring and punishing hackers and malicious cyber states. While a clear policy of active cyber defense may be domestically beneficial, the foreign and international implications of hack back must be understood and, in some cases, mitigated. Based on the analogies considered in this *Backgrounder*, Congress should seek to create an active cyber defense framework akin to constrained private security guards. While more assertive forms of active cyber defense might be desirable in some instances, it would be best to take small steps forward. A limited system for private action would serve as a testing ground to resolve difficult issues while avoiding the major challenges of more aggressive techniques. Once this system is established, Congress can and should revisit it to see whether additional powers and protections can be granted to private companies.

Congress and the Administration should:

- **Permit low-risk active cyber defense measures across U.S. systems.** Congress and the Administration should make clear that low-risk active defense techniques such as information sharing, denial and deception, and hunting activities are permitted under U.S. law.

- **Permit more problematic activities only by certified parties.** The CFAA and the Wiretap Act should be amended to allow private cyber defenders to engage in more aggressive and legally problematic "attribution" activity (such as beaconing or dark web information gathering) only if certified to do so by the DHS. The DHS should create a certification program in consultation with the National Institute of Standards and Technology that provides an assessment for companies to determine whether they are suffi-

29. Jarko, "Finding the Fine Line—Taking an Active Defense Posture in Cyberspace Without Breaking the Law or Ruining an Enterprise's Reputation."
30. Harrington, "Cyber Security Active Defense: Playing with Fire or Sound Risk Management?"

ciently technically proficient and understand the restrictions and limits of their legally permitted activity. These licensed parties should also be granted limited protections from relevant criminal statutes regarding illicit activities that may be unintentionally found on the dark parts of the Internet when researching cyber threats.

- **Explore legal options to protect businesses and individuals that engage in authorized active cyber defenses.** As there are obstacles to active defense in foreign law, the U.S. government should assure cyber private responders that it will shield them from foreign criminal liability so long as they abide by the terms of their license and do not attack foreign systems. This may be of little utility if the company has an international presence, but the U.S. government should explore the ways by which it can defend companies looking to annoy or attribute malicious cyber actors.

- **Seek international cooperation on active cyber defense.** While the U.S. can offer some protections to the private sector for active cyber responses, ultimately, the trans-border nature of the cyber threat means that foreign laws will be involved. The U.S. should work with its allies to promote a system that authorizes U.S. and allied private cybersecurity providers to digitally follow malicious hackers across state lines under certain circumstances and rules. While there will inevitably be cases of friendly fire or collateral damage, the deterrent and punishing effect should be impressed upon U.S. allies in order to come to a cyber self-defense agreement.

Proceeding with Caution

The idea of hack back sounds like something out of a spy novel. What was once the stuff of fiction or imaginative policymaking has become a topic for serious consideration. Multiple organizations and experts, including the Administration-chartered Commission on the Theft of American Intellectual Property, have recommended that consideration be given to easing the domestic American prohibition of active cyber defenses.[31] The system of active cyber defense described in this *Backgrounder* provides the appropriate amount of caution while enhancing the U.S.'s cybersecurity posture.

In the absence of an effective system of cybersecurity provided by the government, it is in some sense immoral to prohibit private-sector actors from protecting themselves. But caution is strongly advised, and while the U.S. government should establish a program for active cyber defense, it also needs to begin building an international consensus regarding private-sector active cyber defense. In addition, while stronger active cyber defense is one way to combat hackers, other levers of national power must also be exercised against campaigns of cyber aggression led by nation-states. The U.S. can and should do more to prevent and stop cyberattacks and espionage; encouraging active cyber defense is but one of the ways to do so.

*—**Paul Rosenzweig** is a Visiting Fellow in the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy at The Heritage Foundation. **Steven P. Bucci, PhD,** who served for three decades as an Army Special Forces officer and top Pentagon official, is a Visiting Fellow in the Douglas and Sarah Allison Center for Foreign Policy, of the Davis Institute. **David Inserra** is a Policy Analyst for Homeland Security and Cyber Policy, in the Allison Center. Portions of this* Backgrounder *appeared in an earlier academic paper by Paul Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures,"* Stanford Journal of International Law*, Vol. 50, No. 103 (Winter 2014).*

31. Commission on the Theft of American Intellectual Property, *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property*, May 2013, http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf (accessed January 13, 2017).