Center for a New American Security

FEBRUARY 2013

Active Cyber Defense
A Framework for Policymakers

POLICY BRIEF

By Irving Lachow

Advanced cyber attacks pose a serious risk to U.S. economic and national security. Passive cyber defenses[1] that rely on perimeter sensors to prevent intrusions cannot adequately protect against increasingly sophisticated cyber attacks. Active cyber defense (ACD), a term that describes a range of proactive actions that engage the adversary before and during a cyber incident, can dramatically improve efforts to prevent, detect and respond to these sophisticated attacks. As a result, ACD activities are becoming increasingly common. One recent survey found that 36 percent of the 180 companies surveyed admitted to engaging in retaliatory hacking at least once – and some people believe that the actual number is much higher.[2]

Yet even as ACD becomes more widespread, the debates about what techniques are appropriate – or even legal – are just beginning. One recent article in *The Washington Post* described ACD as "a controversial and sometimes ill-defined approach that could include techniques as aggressive as knocking a server offline."[3] Many of the public debates on the topic have focused on aggressive aspects of ACD, such as retaliatory "hack-backs" or preemptive hacking.[4] Similarly, a number of cyber security experts and government officials have expressed concerns about companies taking offensive cyber actions through ACD techniques.[5] Furthermore, many companies appear to be unsure about what steps they can and cannot legally take to protect their intellectual and financial resources.[6]

This policy brief aims to inform these emerging debates by providing a framework for thinking about ACD. It begins by describing why ACD is becoming increasingly important. It then examines how ACD can be used by defenders during a timeframe called the cyber engagement zone (CEZ). This zone begins after an attacker has deployed malware on a defender's system and ends when the attacker begins to take specific actions, such as stealing information from the defender. This brief then describes the specific ACD options available to companies within the CEZ and examines the possible legal and operational issues associated with these options.

Why Active Cyber Defense is Needed

The changing nature of cyber threats has made ACD increasingly important in both the private and public sectors. The main threats no longer come from teenage hackers or petty criminals,

although such actors are still around. Instead, sophisticated criminals and state-sponsored spies pose the most danger for businesses and governments.[7] These aggressors primarily focus on stealing intellectual property and defrauding individuals and businesses.[8] The term "advanced persistent threat," or APT, is often used to describe state-sponsored cyber spies who deliberately target specific organizations, use sophisticated means to penetrate those organizations and evade detection within those organizations for weeks, months or even years in order to gather information. This brief focuses primarily on the APT because of the unique challenge it poses to current cyber defenses and the level of harm it could cause to U.S. security, but many of these issues apply equally well to threats from other actors, including cyber criminals and hacker groups like Anonymous.

Passive cyber defenses simply cannot address this threat. As one commentator has noted, the APT is "first and foremost a new attack doctrine built to circumvent the existing perimeter and endpoint defenses."[9] Passive defenses do provide some benefits in this environment; basic cyber hygiene practices, such as patching vulnerabilities, can help to reduce the number of low-level attacks that cyber defenders need to address.[10] Passive defenses are a necessary component of a well-designed cyber defense program, but they are no longer sufficient to address increasingly sophisticated threats. For example, Mandiant's most recent threat report found that:[11]

Only 6 percent of organizations detect advanced attackers via internal methods. Targeted attacks continue to evade preventive defenses. During 2011, the vast majority of targeted organizations – 94 percent – learned that they were victims of cyber attacks from an external entity such as law enforcement.

The typical advanced attack goes unnoticed for more than a year. Once inside a victim organization, attackers typically have plenty of time to reach their ultimate objective – such as stealing intellectual property or financial assets. The median number of days from the first evidence of compromise to identification of the attack was 416 days.

Passive defenses are a necessary component of a well-designed cyber defense program, but they are no longer sufficient to address increasingly sophisticated threats.

Malware only tells half of the story. Organizations' investments in malware detection and antivirus capabilities – although effective at detecting characteristics associated with common worms, botnets and drive-by downloads – do little to help defend against targeted intrusions.

Financially motivated attackers are increasingly persistent. Organized crime groups are adopting persistence mechanisms, such as replacing strains of malware to avoid detection, previously used by the APT.

Numerous other industry reports have reached similar conclusions.[12] Meanwhile, several U.S. government reports have highlighted cyber espionage and criminal activity as significant risks to U.S. economic and national security. For example, the U.S. Defense Security Service commented in a recent report:

> Every time our adversaries gain access to sensitive or classified information and technology, it jeopardizes the lives of our warfighters, since these adversaries can exploit the information and technology to develop more lethal weapons or countermeasures to our systems. Our national security is also at risk in the potential loss of our

> technological edge, which is closely tied to the economic success of the cleared contractor community and the well-being of our economy.[13]

General Keith Alexander, the head of the National Security Agency and U.S. Cyber Command, has called the theft of intellectual property through cyber espionage "the greatest transfer of wealth in human history" and estimates that it costs the United States approximately $340 billion per year.[14] The British government has estimated that cyber crime cost its economy approximately $44 billion in 2011, or almost 2 percent of the British gross domestic product (GDP), mostly due to cyber espionage and theft of intellectual property.[15] The equivalent effect on the U.S. GDP would be about $300 billion and cost roughly 2 million jobs.[16] Other estimates are lower but still extremely consequential, including losses of tens of billions of dollars and hundreds of thousands of jobs.[17]

Given these effects, it is not surprising that both government and industry are using ACD capabilities to augment their passive cyber defenses. As then-Deputy Secretary of Defense Bill Lynn stated in 2011, "It is not adequate to rely on passive defenses that employ only after-the-fact detection and notification. We have developed and now employ a more dynamic approach to cyber defense."[18]

Active Cyber Defense and the Cyber Engagement Zone

As noted earlier, there is no commonly accepted definition of the term "active cyber defense." The only formal definition appears in the 2011 *Department of Defense [DOD] Strategy for Operations in Cyberspace*:

> Active cyber defense is DoD's synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It builds on traditional approaches to defending DoD networks and systems, supplementing best practices with new operating concepts. It operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems. As intrusions may not always be stopped at the network boundary, DoD will continue to operate and improve upon its advanced sensors to detect, discover, map, and mitigate malicious activity on DoD networks.[19]

Many people interpret this definition as referring to technical countermeasures, particularly because DOD has developed sophisticated sensors to detect malware. Although such technologies are an important element of ACD, they are only one aspect of a larger whole. ACD can best be understood as a set of operating concepts that all involve taking the initiative and engaging the adversary in some way.

Advanced cyber attacks do not involve a single discrete event. Instead, aggressors must undertake several steps to accomplish their mission. A particularly useful framework for understanding how APT actors operate is called the cyber kill-chain (CKC).[20] As shown in Figure 1, the CKC divides attacks into seven phases:

1. Reconnoiter. The adversary researches, identifies and selects its targets. This is often done by crawling websites.

2. Weaponize. The adversary couples a piece of malware with a delivery mechanism, such as a Microsoft Office or Adobe Acrobat file. This coupling is often done using an automated tool.

3. Deliver. The adversary transmits the weaponized payload to the target, often through email, websites and USB tokens.

4. Exploit. The malware delivered to the target is triggered when a user takes an action, such as opening an email attachment or visiting an infected website.

FIGURE 1: SEVEN PHASES OF THE CYBER KILL-CHAIN

5. Install. The malware infects the user's system. It may take steps to hide itself from malware detection software on that system.

6. Command and Control. The malware sends an update on its location and status to a command and control server. It often does so through encrypted channels that are hard to detect. The adversary can then command the malware to take specific actions, such as spreading throughout the enterprise or looking for specific types of information.

7. Act. The malware takes actions that accomplish the adversary's objectives. Adversaries usually exfiltrate data from the targeted organization, but they could also alter or destroy data.[21]

Although defenders can respond to an adversary's behavior at any point in the CKC, organizations do not usually engage with attackers until Phase 3 (Deliver), when attackers try to deploy malware on their systems. This is true for two reasons. First, it is technically difficult for a targeted organization to detect and prevent adversaries from conducting reconnaissance, which is basically open-source information gathering. This is usually legal and can often look like legitimate web-based research. It can be very difficult to distinguish between an adversary attempting to mine information about a particular employee and, for example, a prospective job applicant doing homework before an interview, and the risks of miscalculation are high.

It is even more difficult to detect and stop weaponization before an attack is launched. Since the adversary will weaponize the payload from a computer that he or she owns or controls, the only way for a potential victim to know that an adversary is taking such actions is to have access to an adversary-controlled computer. Private-sector organizations do not have the legal right – and most do not have the means – to identify and access these adversary-controlled computers before a specific cyber incident occurs.

Once adversaries have deployed malware on a target in Phase 3, the options for employing ACD techniques grow significantly. This cyber engagement zone, which includes Phases 3 through 7, is where the defender can most easily take the initiative in order to detect the attack, block the attack, gain information about the attackers and their methods, mislead the attackers and possibly even deter them from future attacks. However, organizations often do not know that they have been compromised until Phase 6 (Command and Control), when the installed malware begins communicating outside of the enterprise.[22] By then, the adversary has delivered its weapon, triggered its malicious code and infected the target system.

To illustrate the range of ACD options available in the CEZ, Figure 2 depicts a simple scenario of a cyber attack against a notional organization called Company A. An adversary has taken over a computer in Organization Z, and this computer is

now acting as a command and control (C2) server for attacks on other targets.[23] The C2 server is now issuing instructions to – and possibly receiving stolen data from – an infected machine in Company A (called "Target" in this example). In this scenario:

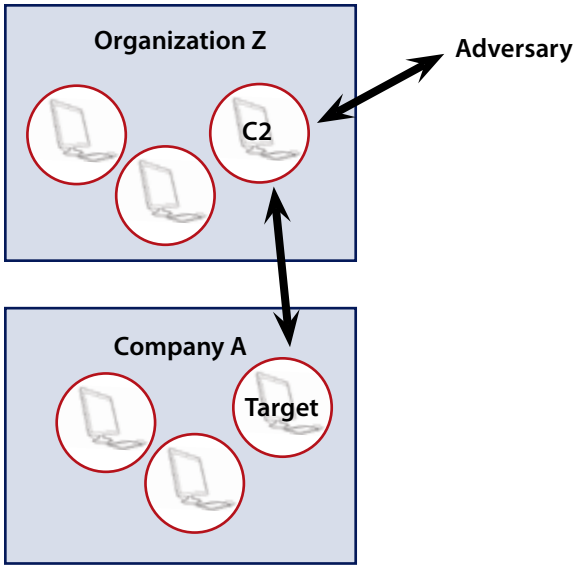
- Organization Z may be an innocent third party that has no idea it has been compromised and is being used to launch cyber attacks.
- Organization Z may be inside or outside the United States. The adversary will often launch attacks against U.S. organizations using C2 servers located in the United States, but this is not always the case.[24]
- The adversary may be directly connected to the C2 server, or there may be numerous intermediate connections between those running the attack and the C2 server. Advanced attacks usually involve multiple intermediate connections.
- The C2 server may be directing numerous cyber attacks. For example, infected computers in Companies B, C and D (not shown in the diagram) may all be communicating with that server.

Company A might respond to this attack using as many as three ACD concepts: detection and forensics, deception and attack termination. This section focuses solely on the operational possibilities of these concepts; the following section addresses the legal debates surrounding such activities.

DETECTION AND FORENSICS

Companies may use a number of ACD techniques to detect attacks that can circumvent passive defenses. One approach uses honeypots to attract adversaries and look for patterns of behavior (often called tactics, techniques and procedures, or TTPs) that may be hallmarks of a specific aggressor.[25] Once Company A detects a cyber intrusion, it will then attempt to gather the following information about the attack:

FIGURE 2: A CYBER ATTACK SCENARIO



- What type of attack has occurred? Types of attack can range from cyber espionage and cyber crime to terrorism and hacktivism.
- How much damage has been done? Has any information been stolen? If so, what information? Has data within the organization been altered or destroyed? Have funds been taken?
- Who is behind the attack? A teenage hacker? A criminal organization? A nation-state?

The process of answering such questions in a formal and rigorous way is called forensics,[26] and the answers will inform Company A's decisions about how to respond.[27] Companies can gather this information in two ways: by focusing their efforts within their own organization (local information gathering) or by reaching out beyond their organization (remote information gathering).

Local Information Gathering

Companies may employ a number of ACD techniques within their own enterprises to gather information about a specific cyber incident. For

example, they can attempt to detect and track adversaries as they explore corporate networks. If a honeypot is set up with a number of different types of documents, corporations can watch to see which documents, if any, the adversary chooses to exfiltrate. This may provide clues about the adversary's motives and may also help to identify the adversary, especially if the company has been able to obtain strategic intelligence on the operational practices of different actors.[28] For example, Company A may know that a particular adversary is looking for information about a specific technology. If documents (real or fake) about that technology are targeted within the enterprise, then the company will gain some evidence (albeit circumstantial) about the identity and motives of the attacker.

Remote Information Gathering

In some cases, an organization may want to gather information about a cyber incident by looking outside of its own borders. For example, a number of ACD techniques will allow Company A to gain access to the C2 server in Organization Z.[29] Once it has access to that server, Company A has the ability to take any number of actions, including scanning the computer, loading software on it, removing data, encrypting data, deleting data and stopping the computer from functioning. Company A can also gather information remotely by tracking documents that have been stolen or copied. This could be accomplished in a number of ways, from placing passive watermarks on files to adding beacons that actively emit a signal when they leave the enterprise. Company A might even be able to create files that "self-destruct" under a specific set of circumstances.[30]

DECEPTION

Deception is an integral part of both offensive and defensive cyber operations.[31] The vast majority of APT attacks are based on deception: attempting to trick users into opening infected files or going to compromised websites. However, deception is not merely a tool for offensive operations; it can serve to strengthen computer defenses as well. Company A could protect its intellectual property through a cyber deception campaign, allowing the adversary to steal documents that contain false or misleading information.[32] The goal of such a campaign would be to deter future cyber attacks by changing the adversary's cost-benefit calculations.[33] Deceptive information could increase the aggressor's costs by requiring more time to analyze and assess the validity and utility of stolen information. It would also potentially lower the benefits of the attack because of uncertainty about the value of the stolen data; the adversary would not know if the stolen information was useful or deliberately designed to be misleading.

Deception poses a number of operational obstacles, however. For example, Company A must be careful that the adversary does not detect its deception campaign. If such a campaign were detected, the adversary could then launch its own deception campaign against Company A and deliberately mislead the company about its TTPs and intentions. In addition, Company A could be harmed if the misleading information were accidently released into the open. For example, if the leaked information contained deliberate errors designed to reduce the value of the information to the attackers and these errors were identified in the leaked information, then Company A might be viewed as producing low-quality products. Nevertheless, the benefits of deception may well outweigh these operational risks.[34]

ATTACK TERMINATION

ACD concepts can also be used to stop a cyber attack while it is occurring. For example, Company A may want to prevent information from leaving its network or to sever the connection between the infected computer within its network and the

C2 server. More aggressive actions might include patching unwitting computers outside of Company A's network that are being used to launch attacks, taking control of remote computers to stop attacks and launching denial-of-service attacks against attacking machines.[35] In the scenario above, many, if not all, of these actions would likely be focused on the C2 server in Organization Z.

Legal Issues Surrounding Active Cyber Defense

Although the three ACD concepts described above are technologically possible, it is not clear whether they are legal. In order to understand the main legal issues that might apply to these ACD techniques, this policy brief focuses on the primary law that applies in such situations: the Computer Fraud and Abuse Act (CFFA) of 1984.[36]

A defendant can violate the CFAA by accessing a "protected computer"[37] without authorization or by exceeding authorized access. In general, the concept of accessing a computer without authorization applies to those outside of a given organization; this is the prototypical hacking scenario in which someone accesses a computer without permission. The concept of exceeding authorized access usually applies to insiders who have obtained or altered information on a computer beyond the authorization that they have been granted. For example, this would apply if an employee deliberately accessed financial data that he or she was not authorized to see.[38] The provisions of the CFAA apply even if Organization Z is located outside the United States.[39]

In the scenario above, if one views Company A and Organization Z as having two totally separate networks, and if Organization Z has not given Company A permission to access to its systems, then any attempt by Company A to access or alter information on the C2 server (which is a part of Organization Z) would violate the CFAA's "without authorization" clause. That is why ACD options that involve retaliation or other types of "hacking back" are generally considered illegal.

However, it may be possible to interpret the scenario differently. At some point in the attack process, the C2 server within Organization Z and the infected computer within Company A will establish a link. At that point, it could be argued that the C2 server has connected to Company A's enterprise and, in doing so, has consented – implicitly if not explicitly – to whatever acceptable use policy Company A has in place.[40] If the acceptable use policy requires the user to forfeit expectations of privacy, consent to monitoring, meet all corporate security requirements or abide by prohibitions on illegal copying of information, then Company A may have the authority to take certain actions that would otherwise be considered illegal.[41]

One could also argue that the common law principle of necessity applies here and gives Company A the right to take actions to defend itself, even if such actions violate the terms of the CFAA or other laws.[42] In this case, Company A would stipulate that taking a specific action to defend itself, such as accessing the C2 server without authorization, is justified because this action yields a greater good to both the company and society than would a strict adherence to the laws that prohibit this action. For example, Company A could argue that determining whether its information had been stolen and gathering information on the adversary that could be provided to government officials would be more beneficial than simply informing law enforcement officials of a possible breach and waiting for a response.

Of course, other legal arguments could be made as well. First, it is possible that neither the "implied consent" argument nor the "necessity" argument would hold up in a court of law to grant Company A the legal right to access the C2 server. Second,

even if the "implied consent" argument granted Company A the authority to access the C2 server in Organization Z, Company A's actions could still be limited by the "exceeds authorized access" clause. Third, accessing the C2 server in Organization Z could violate a number of privacy laws and expose Company A to civil actions as well as criminal prosecution. Fourth, if Organization Z is in another country, then Company A may be found guilty of violating that country's national laws even if it does not violate the CFAA.[43]

These complicated and as-yet-unresolved legal issues deserve more attention in the ACD debate. In particular, it is helpful to think about various ACD activities as falling along a legal continuum that ranges from those with no apparent legal issues to those that clearly violate a law. At one end of the continuum, for example, it seems legal for Company A to take a number of ACD measures within its own networks and systems. It can deploy honeypots, actively track adversaries' movements, use deception techniques, watermark documents and terminate connections from the C2 node to compromised machines with relative impunity. Company A can also gather threat information from external sources such as nonprofit organizations, vendors and government agencies – information that can be used to help it proactively detect and respond to APT intrusion attempts.

At the other end of the continuum, some ACD options seem to clearly violate at least the CFAA, if not other laws. In particular, any actions that destroy data on or cause harm to the C2 server or other computers outside of Company A would almost certainly be illegal unless the necessity argument or some other rationale could be used to justify such actions. This is true whether the ACD response occurs before, during or after a given incident.

A legal grey zone lies between these two endpoints that requires much greater attention from

These complicated and as-yet-unresolved legal issues deserve more attention in the active cyber defense debate.

policymakers. For example, although it is unlikely that Company A can legally take actions that harm either the C2 server itself or the data sitting on that server, Company A may be able to gather information or protect its own proprietary information if such actions do not cause Organization Z any harm. This may be what happened in 2010 when Google responded to cyber attacks that it thought might be coming from Asia. According to *The New York Times*, Google was able to "gain access to a computer in Taiwan that it suspected of being the source of the attacks. Peering inside that machine, company engineers actually saw evidence of the aftermath of the attacks."[44] This may also be where the informed consent and necessity arguments carry the most weight: to justify access to the C2 server for the purposes of gathering information.

Although scanning the C2 server in Organization Z may not violate the CFAA, the act of doing that scanning could pose additional legal issues. For example, Company A may come across sensitive information that is protected by other laws, including financial information, personally identifiable information and health care information. Company A could also come across sensitive corporate information that had been stolen from other companies, as happened in the Google case. When Google scanned the computer in Taiwan, it saw evidence of attacks involving "at least 33 other companies, including Adobe Systems, Northrop Grumman and Juniper Networks."[45] As a result, Google "alerted American intelligence and law enforcement officials and worked with them to assemble

powerful evidence that the masterminds of the attacks were not in Taiwan, but on the Chinese mainland."[46]

The Google case may set a precedent of what is allowable, but one could imagine similar scenarios that could lead to civil or criminal charges. In addition, things get more complex if Company A tries to trace a path from the C2 server back to the source of the attacks across multiple organizations (this assumes that the adversary is not directly connected to the C2 server in Organization Z but is several "hops" away). First, accomplishing this kind of trace is technically challenging. Second, even if it were technically feasible, Company A could likely need to cross multiple jurisdictions, and hop through several countries, to trace the source of the attack. In doing so, Company A would potentially violate a number of laws, including state laws within the United States, national laws of other countries and possibly international laws such as the Council of Europe's Convention on Cybercrime.

Another interesting scenario concerns the right of Company A to patch the C2 server connected to its network. Using the informed consent argument, Company A could argue that the C2 server must now comply with its security policies. If the C2 server's configuration did not align with the Company A's requirements, Company A could assert the right to either patch the machine or drop it from the network. The latter would simply terminate the connection between the two organizations, but patching the C2 server would entail deleting or altering information on one of Organization Z's computers. That could be interpreted as a violation of the CFAA. What makes this scenario so interesting is that when the C2 server is connected to Company A, it is technically part of two different networks at the same time. This raises the question of what right Company A has to impose its policies on the C2 server if those policies conflict with the policies of Organization Z. Things are further complicated in this scenario by the fact the C2 server is being directed to connect with Company A by the adversary, not by someone working in Organization Z.

The U.S. government needs to provide greater clarity on which ACD actions are legal and which ones are not.

These complicated and murky legal questions have profound implications for economic activity as well as national security. For example, if Company A has the legal right to scan the C2 server in Organization Z, wouldn't Company A also have the right to scan the machine of a business partner (say, Company B) that is also connected to its network in order to exchange information? And wouldn't Company B have the right to scan Company A's machines as well? How might such a right affect the dynamics of business relationships both within the United States and internationally? Would the security benefits outweigh the possible economic costs?[47]

Conclusion

Active cyber defense concepts are important and potentially necessary tools for countering the increasingly sophisticated cyber threats facing the United States. Companies, like government agencies, are increasingly interested in using such techniques. This policy brief has identified the wide range of ACD options available to private-sector organizations, especially in the cyber engagement zone. Some of these options are almost certainly legal, some are almost certainly illegal and some fall into a grey zone where further guidance is needed.

The U.S. government needs to provide greater clarity on which ACD actions are legal and which ones are not. Without such guidance, two problematic situations may arise. First, organizations may choose not to take actions that are legal because of fears of breaking vague provisions of existing law. Second, organizations may take actions that they believe are legal but that government authorities view as being illegal. In the former case, corporations are bypassing ACD options that could help protect valuable information. In the latter case, companies are taking actions that could lead to serious financial and legal risks and could also undermine U.S. national objectives (such as U.S. efforts to establish norms in cyber space). Clearer guidance will enable organizations to protect themselves from advanced cyber attacks to the greatest extent possible without putting themselves in legal jeopardy.

Dr. Irving Lachow is a Senior Fellow and Director of the Program on Technology and U.S. National Security the Center for a New American Security.

ENDNOTES

1. "Passive defenses" are defined by the Department of Defense as "measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action *without* the intention of taking the initiative" (emphasis added). Department of Defense, *Dictionary of Military and Associated Terms*, Joint Publication 1-02 (April 12, 2001; as amended June 13, 2007).

2. nCircle, "Black Hat Survey: 36% of Information Security Professionals Have Engaged in Retaliatory Hacking," nCircle.com, July 26, 2012, http://www.ncircle.com/index.php?s=news_press_2012_07-26-Black-Hat-Survey-36-percent-of-Information-Security-Professionals-Have-Engaged-in-Retaliatory-Hacking.

3. Ellen Nakashima, "To Thwart Hackers, Firms Salting Their Servers with Fake Data," *The Washington Post*, January 2, 2013, http://articles.washingtonpost.com/2013-01-02/world/36211654_1_hackers-servers-contract-negotiations.

4. For example, see John Reed, "Mike Rogers: Cool It with Offensive Cyber Ops," Killer Apps blog on ForiegnPolicy.com, December 14, 2012, http://killerapps.foreignpolicy.com/posts/2012/12/14/mike_rogers_cool_it_with_offensive_cyber_ops.

5. For example, see Steptoe, "The Hackback Debate," Steptoe Cyberblog, http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/; David Dittrich, "No, Executing Offensive Actions Against Our Adversaries Really Does Have High Risk (Deal with It)," Honeynet Project blog on Honeynet.org, December 10, 2012, http://www.honeynet.org/node/1004; and Jody Westby, "Caution: Active Response to Cyber Attacks Has High Risk," Forbes.com, November 29, 2012, http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk.

6. Author interviews, October and November 2012.

7. Other cyber threats worth noting include denial-of-service attacks against companies and government agencies, attacks that cause the destruction of data and attacks that cause physical equipment to malfunction. The world has seen examples of all three of these attack methods in the past few years, but at present, the risks posed by such methods are not equivalent to the harm caused by criminal and espionage activity.

8. Cabinet Office and Detica, "The Cost of Cyber Crime" (February 14, 2011), 2, http://www.baesystemsdetica.com/uploads/press_releases/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf.

9. Uri Rivner, "Anatomy of an Attack," Speaking of Security blog on rsa.com, April 1, 2011, http://blogs.rsa.com/anatomy-of-an-attack.

10. For example, according to the Australian Department of Defense, "at least 85% of the intrusions that DSD [Defense Signals Directorate] responded to in 2011 involved adversaries using *unsophisticated* techniques that would have been mitigated by implementing the [DSD's] Top 4 mitigation strategies as a package" (emphasis added). These four strategies include application whitelisting, patching and using the latest versions of applications, patching and using the latest versions of operating systems, and minimizing administrative privileges. See Australian Department of Defence, Defence Signals Directorate, "Top 4 Mitigation Strategies to Protect Your ICT System," November 2012, http://www.dsd.gov.au/publications/csocprotect/top_4_mitigations.htm.

11. Mandiant, "M-Trends 2012: An Evolving Threat" (2012).

12. For example, see recent threat reports from FireEye, McAfee, Sophos, Symantec and Verizon.

13. Defense Security Service, *Targeting U.S. Technologies 2012: A Trend Analysis of Reporting from Defense Industry* (November 29, 2012), 5. See also reports from the National Counterintelligence Executive and the U.S.-China Commission.

14. Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History,'" The Cable blog on ForeignPolicy.com, July 9, 2012, http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history.

15. Cabinet Office and Detica, "The Cost of Cyber Crime." The report notes that "the real impact of cyber crime is likely to be much greater" than its estimate.

16. This is based on a U.S. 2011 GDP estimate of $15 trillion and the assumption that 1 percent of GDP translates roughly to 1 million jobs. For more details on the GDP-to-jobs conversion, see Executive Office Of The President Council Of Economic Advisers, *Estimates of Job Creation from the American Recovery and Reinvestment Act of 2009* (May 2009).

17. Ellen Nakashima, "U.S. Said to Be Target of Massive Cyber-espionage Campaign," *The Washington Post*, February 10, 2013, http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html.

18. William J. Lynn, III, "Remarks on Cyber" (RSA Conference, San Francisco, February 15, 2011), http://www.defense.gov/speeches/speech.aspx?speechid=1535.

19. *Department of Defense Strategy for Operations in Cyberspace* (July 2011), 7.

20. This concept was originally presented in Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" (paper presented at the 6th Annual International Conference on Information Warfare and Security, Washington, March 17-18, 2011), http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf. This discussion of the kill-chain concept is also informed by MITRE, Active Defense Strategy for Cyber" (July 2012); and LTG Charles Croom, "The Cyber Kill Chain: a Foundation for a New Cyber Security Strategy," *High Frontier*, 6 no. 4 (August 2010), 52-56, http://www.afspc.af.mil/shared/media/document/AFD-101019-079.pdf.

21. For an example of such an attack, see "Aramco Says Cyberattack Was Aimed at Production," *The New York Times*, December 9, 2012, http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0.

22. Several techniques for detecting malware during this phase are provided in McAfee, "Global Energy Cyberattacks: 'Night Dragon'" (February 10, 2011).

23. The actual human adversary may be directly connected to the C2 server in Organization Z or may be connecting to a number of intermediate computers that lie between him or her and the C2 machine. These intermediate machines make it much harder for Company A, or anyone supporting Company A, to identify and locate the adversary.

24. As noted below, additional legal issues may apply if Organization Z is located outside the United States. For a discussion of reasons why adversaries might want to launch cyber attacks from within the United States, see Robert A. Miller, Daniel T. Kuehl and Irving Lachow, "Cyber War: Issues in Attack and Defense," *Joint Forces Quarterly*, 61 (2011), 18-23.

25. A honeypot is a trap that uses a realistic computer environment to attract and monitor an intruder. For more information on the use of honeypots to detect sophisticated cyber attacks, see Sean Bodmer, Max Kilger, Gregory Carpenter and Jade Jones, *Reverse Deception: Organized Cyber Threat Counter-Exploitation* (New York: McGraw-Hill Osborne Media, 2012); and European Network and Information Security Agency, *Proactive Detection of Security Incidents: Honeypots* (November 20, 2012). The use of TTPs to detect adversary behavior is a key tenet behind the development and use of the cyber kill-chain. See Hutchins, Cloppert and Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains."

26. One definition describes computer forensics as "the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law." See http://searchsecurity.techtarget.com/definition/computer-forensics. Although forensics can refer specifically to the process of gathering evidence for legal actions, this policy brief applies the term more broadly. Here, forensic activity can be performed without directly supporting a formal legal investigation.

27. For an excellent analysis of the role of attribution in ACD, see Shane McGee, Randy V. Sabett and Anand Shah, "Adequate Attribution: A Framework for Developing a National Policy for Private Sector use of Active Defense," *Journal of Business and Technology Law* (forthcoming).

28. This approach was used during the joint investigation by the Information Warfare Monitor and the Shadowserver Foundation of cyber espionage activity in India, the U.N. and the Offices of the Dalai Lama. See Information Warfare Monitor and Shadowserver Foundation, "Shadows in the Cloud: Investigating Cyber Espionage 2.0," JR03-2010 (April 6, 2010), http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0. See also Information Warfare Monitor, "Tracking GhostNet: Investigating a Cyber Espionage Network" (Citizen Lab/The SecDev Group, March 29, 2009).

29. For example, during the GhostNet investigation, researchers monitored infected computers at several organizations and were able to use a packet capture tool to identify the location of the C2 servers used to manage the espionage campaign. See Information Warfare Monitor, "Tracking GhostNet," 14-15.

30. John Markoff, "New Technology to Make Digital Data Self-Destruct," *The New York Times*, July 20, 2009, http://www.nytimes.com/2009/07/21/science/21crypto.html?_r=0.

31. Nakashima, "To Thwart Hackers, Firms Salting Their Servers with Fake Data."

32. Although the misleading information could be put in place before a given cyber attack began, the actual effect would occur during the "Act" phase of the CKC, which is part of the CEZ.

33. Edward Roberts, "Deception and the Art of Cyber Security," *SC Magazine*, February 28, 2012, http://www.scmagazine.com/deception-and-the-art-of-cyber-security/article/229685/.

34. For a detailed discussion of the broader topic of deception, see Michael Bennett and Edward Waltz, *Counterdeception Principles and Applications for National Security* (Boston: Artech House, 2007); and Edward Amoroso, *Cyber-Attacks: Protecting National Infrastructure* (Burlington, MA: Elsevier, 2011), 39-50.

35. See David Dittrich and Kenneth Einar Himma, "Active Response to Computer Intrusions," in *The Handbook of Information Securi*ty, ed. Hossein Bidgoli (Hoboken, NJ: John Wiley & Sons, 2005). A denial-of-service attack attempts to make a computer, network or service unavailable to intended users. This is often accomplished by flooding the target with an overwhelming number of legitimate requests that create a bottleneck or shut down the system.

36. This discussion is based on material found in Office of Legal Education, Executive Office for United States Attorneys, *Prosecuting Computer Crimes*, http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf; and 18 U.S.C. § 1030, "Fraud and Related Activity in Connection with Computers." There are several other laws that could have some relevance for a given ACD scenario, especially the Electronic Communications Privacy Act of 1986. For a description of the "patchwork" of laws that apply to cyber security, see The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (May 2009).

37. A "protected computer" can be interpreted as a computer that is connected to the Internet. See Office of Legal Education, Executive Office for the United States Attorneys, *Prosecuting Computer Crimes*, 4.

38. Recent court decisions have narrowed the scope of this provision to focus on information access rather than use. See Onin Kerr, "Ninth Circuit Hands Down En Banc Decision in United States v. Nosal, Adopting Narrow Interpretation of Computer Fraud and Abuse Act," Volokh.com, April 10, 2012, http://www.volokh.com/2012/04/10/ninth-circuit-hands-down-en-banc-decision-in-united-states-v-nosal-adopting-narrow-interpretation-of-computer-fraud-and-abuse-act/.

39. The CFAA protects "a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." See 18 USC § 1030 (e)(2)(b), http://www.law.cornell.edu/uscode/text/18/1030.

40. This argument is presented in Stevan D. Mitchell and Elizabeth A. Banker, "Private Intrusion Response," *Harvard Journal of Law & Technology*, 11 no. 3 (Summer 1998), note 25, 711.

41. This is another area of contention because of the prosecution of Aaron Swartz under the terms of the CFAA and his subsequent suicide. Taylor Amerding, "'Aaron's Law' Could Have Unintended Consequences," *Network World*, January 18, 2013, http://www.networkworld.com/news/2013/011813--aarons-law-could-have-265944.html.

42. This point was made by Orin Kerr in his debate with Steward Baker. See Steptoe, "The Hackback Debate." A useful summary of the principle of necessity can be found at http://legal-dictionary.thefreedictionary.com/Necessity+defense.

43. This can happen to U.S. government personnel as well. In 2002, an FBI agent was indicted by the Russian government for illegally accessing data on a Russian criminal's computer as part of a sting operation. Mike Brunker, "FBI Agent Charged with Hacking," MSNBC.com, August 15, 2002, http://www.msnbc.msn.com/id/3078784/ns/news-internet_underground/t/fbi-agent-charged-hacking/#.UNip04mfiKw.

44. David E. Sanger and John Markoff, "After Google's Stand on China, U.S. Treads Lightly," *The New York Times*, January 15, 2010, http://www.nytimes.com/2010/01/15/world/asia/15diplo.html.

45. Ibid.

46. Ibid.

47. I am indebted to Andy Grotto for highlighting this dilemma.

I would like to acknowledge the following individuals for their feedback and advice on this policy brief: Stewart Baker, Nora Bensahel, Richard Bejtlich, Robert Butler, Steve Chabinsky, Richard Danzig, Gary Gagnon, Frank Kramer, Randy Sabett and Jacob Stokes.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. The views expressed in this report are those of the authors and do not represent the official policy or position of the Department of Defense or the U.S. government.

Center for a New American Security
1301 Pennsylvania Avenue, NW
Suite 403
Washington, DC 20004

TEL 202.457.9400
FAX 202.457.9401
EMAIL info@cnas.org
www.cnas.org

Contacts
Kay King
Senior Advisor and
Director of External Relations
kking@cnas.org, 202.457.9408

Sara Conneighton
Deputy Director of External Relations
sconneighton@cnas.org, 202.457.9429

Cover image by iStock photo.