The US Army War College Quarterly: Parameters

Volume 44
Number 3 *Parameters Autumn 2014*

Article 12

Fall 9-1-2014

Hacking Back: Not the right Solution

Emilio Iasiello

Recommended Citation
Emilio Iasiello, "Hacking Back: Not the right Solution," *Parameters* 44, no. 3 (2014), doi:10.55540/0031-1723.2732.

Hacking Back: Not the Right Solution

Emilio Iasiello

Abstract: In cyberspace attackers enjoy an advantage over defenders, which has popularized the concept of "active cyber defense"—offensive actions intended to punish or deter the adversary. This article argues active cyber defense is not a practical course of action to obtain tactical and strategic objectives. Instead, "aggressive cyber defense," a proactive security solution, is a more appropriate option.

The ability to retaliate against cyber attackers—irrespective of the legalities of such actions—appears to have gained traction in the United States government, but is it a practical response for achieving tactical and strategic objectives in cyberspace? Attribution limitations, collateral damage considerations, the Internet's global architecture, and potential event escalation make the challenges of engaging in active cyber defense an ineffective course of action destined to achieve limited tactical successes at best; and it risks accelerating digital as well as physical conflict. Too many variables prevent active cyber defense deterring or punishing adversaries in cyberspace. For that reason, this article advocates a more productive solution—aggressive cyber defense—to frustrate attackers via nondestructive or damaging activities.

A Note on Terminology

There are no internationally accepted definitions for "cyber attack" and "active cyber defense." In its 2011 *Strategy for Operating in Cyberspace,* the US Department of Defense defines active cyber defense as:

> . . . synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities . . . 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.[1]

Using this designation as a baseline, the following definitions have been adopted for the purposes of this article:

- **Cyber Attack**: Actions ranging from network exploitation for information collection/data theft to attacks designed to deny, degrade, disrupt, or destroy an information system, an information network, or the information resident on them. Examples include distributed denial-of-service attacks, the insertion of malware designed to destroy information systems, or the information resident on them such as Stuxnet or Shamoon.
- **Active Cyber Defense**: A range of offensive *damaging or destructive* actions, such as counterhacking, that engage an adversary during or

Emilio Iasiello has been a cyber-threat analyst for the past twelve years supporting the US Departments of State and Defense, as well as a private sector security firm.

[1] US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: US Department of Defense, July 2011); http://www.defense.gov/news/d20110714cyber.pdf.

promptly after an initial cyber attack. Active cyber defense does not include nonviolent actions such as diplomatic or economic sanctions. Examples include counterhacking and technical countermeasures with weaponized payloads.

- **Passive Cyber Defense**: A range of cyber defensive actions taken to protect the confidentiality, integrity, and availability of information systems and networks through the use of layered network security devices, processes, and countermeasures to protect the integrity of the information assets in an enterprise. Examples include firewalls, intrusion detection systems, and host-based intrusion detection systems.
- **Aggressive Cyber Defense**: A range of aggressive passive and active defensive actions to be used in concert with one another that identify, deceive, and frustrate attackers into giving up and moving elsewhere. Examples include severing connections between targeted computers and the attacking command and control servers, as well as redirecting hostile traffic to a benign target or destination.

Active Cyber Defense

The United States faces increasing cyber threats capable of targeting private and public sectors from a diverse actor set. Director of US National Intelligence James Clapper identified cyber as the top threat facing the United States, over traditional high profile threats such as terrorism and weapons of mass destruction.[2] Cyber crime, hacktivist-related distributed denial-of-service attacks, and cyber espionage have prompted policymakers to develop deterrence strategies. The United States, as well as the governments of Canada,[3] France, Germany, and the United Kingdom, have developed and published cybersecurity strategies acknowledging the severity of this threat, as well categorizing the actors suspected of perpetrating it.[4]

Opponents of passive cyber defense quickly point out there has been limited success in mitigating hostile activity via conventional cyber defense practices. Active cyber defense seemingly remains the only real solution to deter or stop aggressive cyber actors.[5] This concept is not new; the cybersecurity research community has discussed active cyber defense for nearly a decade.[6] However, for it to be effective, an active cyber defense program must be able to:

[2] Director of National Intelligence, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, James R. Clapper, Director of National Intelligence* (Washington, DC: Office of the Director of National Intelligence, January 29, 2014).

[3] Government of Canada, *Canada's Cyber Security Strategy*, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

[4] The White House, *International Strategy for Cyberspace* (Washington, DC: The White House, May 2011);Governmentof Canada, *Canada's Cyber Security Strategy*, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.; *Agencie Nationale de la Securite des Systemes d'Information, Information Systems Defence and Security* – France's Strategy, http://www.ssi.gouv.fr /IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf; Federal Ministry of the Interior, *Cyber Security Strategy for Germany*, http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf;jsessionid=065625A05192FE06B3F0C34A89E935B3.2_cid093?__blob=publicationFile; Government of the United Kingdom, *The UK Cyber Security Strategy*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

[5] Ellen Nakashima, "Cybersecurity Should Be More Active, Official Says," *Washington Post*, September 16, 2012.

[6] Jody Westby, "Caution: Active Response to Cyber Attacks Has High Risk," *Forbes.com*, November 11, 2012.

1. Correctly identify the originator of the cyber attack or an impending cyber attack
2. Determine why the attack happened or will happen and be prepared to launch a cyber response with commensurate power and effect

A retaliatory action should cause more harm than the original attack, and as a result, thereby deterring or halting an attack. But can such a goal be obtained?

Certain conditions must be in place prior to implementing active cyber defense. First, a state must have, and communicate to, the international community that it has a red line for tolerance of hostile cyber activity against its networks. Equally important is that this threshold be manageable; a state must be able to deliver on a promised reprisal. For example, a zero-tolerance policy is unfeasible in an age where the volume of hostile cyber activity ranges from aggressive network scanning, to surreptitious network exploitation, to assertive distributed denial-of-service attacks from the large and diverse threat actor landscape.[7] A state could exhaust personnel and financial resources very quickly trying to address every possible threat.

Second, and a corollary to communication, is signaling. Whether in peacetime or war, a key element of any active cyber defense strategy includes the ability to signal intentions to the receiver properly. Without the ability to signal, active cyber defense runs the risk of being misunderstood or misinterpreted, increasing the danger of conflict escalation. What's more, the signaling nation must have established credibility conducting successful and destructive cyber retaliation. If the adversary does not believe the credibility of a signaling state, signaling efforts will fail.

The third necessary condition is the capability to deliver an appropriate cyber response. Proper proportionality eliminates the need to "kill a cockroach with a rocket launcher" when simply stepping on it would suffice. A disproportionate response runs the risk of escalating conflict. Fourth, a state must determine if the cyber attack was intentional and not a mistake, a misunderstanding, or the result of collateral damage. Fifth, and perhaps most important, a state must determine attribution and be willing to accept the risk of being wrong.

Attribution is not easy. Several technical measures as well as operator tactics, techniques, and procedures readily obfuscate a hostile cyber actor's true country of origin. Anonymizers, proxies, and the use of a series of compromised computers in different countries or "hop points" all impede technical attribution. Furthermore, operational security measures and an increasingly sophisticated malware environment (such as multi-functional rootkits) pose real challenges to identifying individuals conducting nefarious activities. Prior to engaging active cyber defense, attribution must be conclusive to ensure the right target is in the cross hairs and the initial attack was intentional. Therein lies the heart of the problem—the ability to identify the intent and identity of the attacker conclusively.

Antagonistic cyber actors can be cast into two categories: the opportunistic hacker and the focused hacker. The former will take advantage

[7] Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009).

of a vulnerability and attempt to exploit it regardless of the target; whereas the latter—whether a state or those actors working on behalf of one—identifies specific targets to exploit. While the tactical objective of active cyber defense is the original attacker, the strategic objective is the decision maker—whether the leadership of a government or a group of nonstate actors. Therefore, active cyber defense must achieve two objectives: 1) make adversarial efforts economically or punitively impractical so they stop, and presumably, go on to another target; and 2) cause the decision making authority to stop directing the hostile activity.

In its 2011 strategy, the Department of Defense determined hostile cyber activity included the persistent theft of proprietary information as a justified reason to conduct active cyber defense.[8] However, there are several challenges and potential pitfalls to engaging in this type of cyber retaliation, even if governments focus efforts exclusively on actors engaged in sophisticated cyber attacks:

- **Multiple Computers**. One goal of active cyber defense is to touch the adversary's computer digitally. But this rationale appears predicated on assuming the attacker has access to, or only uses, one computer. If resourced by a foreign government, it is extremely likely actors will have more than one computer at their disposal. Should an active cyber strike destroy one computer, the others could continue. A second computer would have a new IP address, and attackers could route their activities through a different infrastructure, thus compromising the defender's ability to track their movements. In this instance, the tactical objective—"hurting" the attacker is achieved, but with limited strategic value.
- **Collateral Damage.** The networked environment is notoriously unsecure and has historically fallen victim to intentional and unintentional malware spills. Given that key servers may be optimum targets in cyberwarfare, the possibilities for collateral damage increase, especially if these servers host important civilian emergency services, hospitals, or schools. While some may believe some cyber weapons will have safeguards to prevent collateral damage, historical and current examples say differently.[9] Suspected of having been developed by nation states,[10] Stuxnet was a computer virus designed to target specific configuration requirements in Siemens software resident on the centrifuges of the Iranian nuclear facility at Natanz. However, the virus escaped, infecting computers in Azerbaijan, Indonesia, India, Pakistan, and the United States.[11] Another sophisticated cyber weapon called Flame was designed to spread to other systems over a local network or via USB drive, with the ability to record audio, capture screenshots, log keyboard activity, and network traffic.[12] Although the

[8] US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: US Department of Defense, July 2011).

[9] David Raymond, Gregory Conti, Tom Cross, and Robert Fanelli, *A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons*, http://www.ccdcoe.org/publications/2013proceedings/d1r2s6_raymond.pdf

[10] Nate Anderson, "Confirmed: U.S. and Israel Created Stuxnet, Lost Control of It," *ArsTechnica*, June 1, 2012.

[11] Symantec,"W32.Stuxnet,"http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

[12] Aleks, "The Flame: Questions and Answers," Secure List, May 28, 2012, https://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers.

apparent targets of this malware were computers in the Middle East, Flame also propagated outside that area. Microsoft suffered some collateral damage from Flame, which exploited a previously unknown flaw in the company's digital certificates to disguise malicious code as a Microsoft product. The software firm subsequently issued an update to block other hackers from abusing the fraudulent certificates.[13] In 2012, the US Department of Defense signed a directive limiting any collateral damage from dangerous robotic instruments to "minimize the probability and consequences of failure." Yet, while the directive was set up to create these safeguards, it explicitly "does not apply to autonomous or semi-autonomous cyberspace systems for cyberspace operations."[14]

- **Escaping into the Wild.** An ancillary concern to collateral damage is having malware circumvent any existing controls and spread across the Internet. While this effect may not be the intent of a cyberweapon, when malware interacts with already imperfect information systems, the potential for undesired effects cannot be overlooked or underestimated. The 1988 Morris Worm, according to its creator, was not designed to cause damage, but to gauge the size of the Internet.[15] Regardless, the worm's creators lacked knowledge concerning its potential propagation rate; incomplete testing thus caused the worm to replicate much faster than anticipated, infecting approximately 60,000 machines.[16] If the cyber weapon is self-propagating, like a worm or virus, then the possibility of it "escaping" remains a real concern, despite controls. After all, Stuxnet was never intended to travel outside Natanz's air gapped networks, but an error in the code caused the worm to replicate itself when an Iranian technician connected an infected laptop computer to the Internet.[17] One source claimed the worm spread to at least five countries and as many as 115, including a Russian nuclear plant.[18]
- **Friendly Fire**. Active cyber defense assumes the attacker is actually operating from within a certain state's borders. Should active cyber defense be successful, adversary nations may relocate their operators globally and alter their methods of operation. This response would give attackers the advantage of "disappearing" into the ether as technical and operational data become obsolete. Compounding problems would occur if attackers operated from not only a third-party country, but an allied or friendly one. This possibility leads to difficult questions: Can the defender legally and morally attack the infrastructure of allied or third-party nations without the consent of the host government? Should the defender strike the attacking cyber operator, or the government directing the attack? How will the defender determine if

[13] Aliya Sternstein, "U.S. Moves to Contain Collateral Damage from Cyber Weapons," *Nextgov,* June 19, 2012.

[14] "Pentagon Strips Collateral Damage Safeguards from Cyberwar Weapons," *RT.com*, November 28, 2012.

[15] Craig Wright, "What the Law Says About Distributing a Virus," *Infosec Island,* September 20, 2011.

[16] Carolyn Marsan, "The Morris Worm Turns 20: Look What It's Done," *Network World*, October 30, 2008.

[17] Vincent Manzo, "Stuxent and the Dangers of Cyberwar," *National Interest* (January 29, 2013), http://nationalinterest.org/commentary/stuxnet-the-dangers-cyberwar-8030.

[18] Vivian Yeo,"Stuxnet Infections Continue to Rise," *ZD Net*, August 6, 2010; John Leyden, "Rogue US-Israel Cyber Weapon Infected Russian Nuclear Plant," *The Register*, November 11, 2013..

whether the government was in fact guiding the attacker?

Two examples underscore the impracticality of active cyber defense within this context. The first involves the 1998 distributed denial-of-service attack against Georgia, when the Russian government was suspected of being involved.[19] Technical analysis by Arbor Networks indicated computers in several countries were used, suggesting a botnet attack.[20] Based on this information, where should a defender direct an active defense action? A similar example involved GHOSTNET, a large cyber espionage campaign exploiting computers in 103 countries, particularly those of ministries of foreign affairs and embassies. Should a defender strike back at hosting or command and control servers in other countries, thereby encroaching on the sovereignty of a third party? In both examples, active cyber defense does not seem feasible.

- **Attacker Uses Victim Country**. Here, the aggressor initiates attacks from within the victim country and routes through several hop points before coming back to the target. This approach would take advantage of governments' notoriously horrible bureaucracies and failures of intelligence and security services to collaborate. By the time confliction is resolved, the attackers have most likely relocated to another country to resume operations. Additionally, operating out of a victim country nullifies technical analysis linking attackers with governments based on "office hours" and holidays.
- **Risk of Counter-Strike . . . and Escalation**. There is a real possibility active cyber defense will not deter attackers and, in fact, will invite a stronger counterattack against more valuable systems. This is a dangerous scenario; it runs the risk of conflict escalation, particularly if the attacker perceives the active cyber defense response as disproportionate to the initial attack. Furthermore, a quick and efficient counterattack reveals to the attacker a sense of the defender's capabilities, attribution processes, and the types of tools the defender has at his disposal. Further complicating matters, if the attribution was incorrect, the retaliating government could strike the wrong target, particularly if hasty action is taken.
- **Nonstate Actors.** Terrorist groups, hacktivists, and cyber criminals tend to operate in areas with limited legal restrictions, or government interference. For example, in 2007, after it was determined pro-Kremlin Russian hacktivists originated distributed denial-of-service attacks against Estonia, Tallinn submitted requests to Moscow for assistance in tracking the perpetrators—which were refused.[21] If Estonia chose to conduct retaliatory strikes against Russian interests, it ran the risk of escalating the crisis. Another iteration of this scenario involves a nonstate actor operating from a third-party country, neither allied nor friendly with the victim country. By retaliating against the nonstate actor, the victim country would encroache on the sovereignty of the third country. Even if the retaliation was successful, it is not clear it would achieve any noticeable effect. Assuming extradition is unlikely, and the actor is essentially shielded by the laws of the host country,

[19] Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986-2012* (Vienna: Cyber Conflict Studies Association, 2013), 202-203.

[20] Jose Nazario, "Georgia DDoS Attacks–A Quick Summary of Observations," *Arbor Networks*, August 12, 2008.

[21] Eric Talbot Jensen, "Cyber Deterrence," *Emory International Law Journal*, 26 (2012): 805.

it would be difficult to deter the actor from future activity. Tactical success (hacking back, destroying the computer, etc.) would not translate into strategic victory.

Aggressive Cyber Defense—One Possible Solution

It is highly unlikely any organization can stop all hostile cyber activity targeting its information systems. However, it is wrong to think passive cyber defense has been a failure. Based on multiple surveys, standard defense-in-depth principles have a valid place in computer security, particularly in countering the significant volume of "known" cyber threats. Many companies are still not consistent with implementing the most basic of security procedures. According to one survey, only 45 percent of responding companies believed they were doing well, and of that, only 10 percent were taking adequate security steps.[22] The following points highlight how, if adhered to, most basic security practices are able to mitigate the vast majority of malicious cyber activity an organization encounters on a day-to-day basis:

- An internationally recognized information security vendor SANS, developed the fourth iteration of its "Twenty Critical Security Controls for Effective Cyber Defense (CSC)," baseline security measures addressing the most common hostile cyber activities.[23] For those organizations properly implementing the CSC, there have been encouraging signs of success in the reduction of known threats. In 2009, the US Department of State Chief Information Officer implemented the CSC and found 88 percent reduction in vulnerability-based risks against 85,000 systems.[24] In a 2013 survey, 25 percent of 699 respondents from companies ranging from 100 employees to Global 200 stature were able to quantify improvement in their respective risk postures after implementing the CSC.[25]
- In 2011, the Australian government's Defence Signals Directorate (DSD) published a revision of its "Strategies to Mitigate Targeted Intrusions" designed for advanced persistent threat activities. The strategies listed therein focused on basic information security principles such as patch applications, whitelisting, minimizing the number of users with administrative privileges, filtering, user education, host-based and network intrusion detection systems, to name a few. According to the Australian DSD's findings, the strategies would have prevented at least 70 percent of the intrusions the DSD analyzed in 2009, and at least 85 percent of the intrusions responded to in 2010.[26]

A needed step forward is shifting the mindset of security personnel from passive cyber defense to an aggressive cyber defense; the difference is the latter focuses on proactive defensive measures to mitigate lesser sophisticated attacks (using conventional cybersecurity devices such as

[22] James A. Lewis, *Raising the Bar for Cybersecurity* (Washington, DC: Center for Strategic & International Studies, February 12, 2013).

[23] SANS Institute, "CSIS: 20 Critical Security Controls," http://www.sans.org/critical-security-controls.

[24] SANS Institute, "A Brief History of the 20 Critical Security Controls," http://www.sans.org/critical-security-controls/history.

[25] John Pescatore, "SANS 2013 Critical Security Controls Survey: Moving from Awareness to Action," June 2014.

[26] Government of Australia, *Strategies to Mitigate Targeted Cyber Intrusions*, February 2014.

intrusion detection systems, firewalls, and antivirus programs), enabling security professionals to concentrate on more sophisticated cyber threats. The objective is to build stability through a strong defensive posture placing emphasis on aggressiveness in defense, not on offense. Through a combination of strategy, policy, and defensive tactics, techniques, and procedures, attackers' success rates should decrease; defenders' ability to improve upon resiliency will increase, and the costs associated with cleaning up after cyber incidents will be greatly reduced.

- **Mitigating Targeted Intrusions**. Make it extremely difficult for all but the most dedicated and persistent adversary to continue hacking. This serves two goals. First, it deters most attackers looking to target networks; the theory is there are easier targets to go after. Second, it will be easier to attribute attackers who are able to intrude on networks since such intrusions will require a certain level of sophistication and skill. Combining cognitive and behavioral analyses with technical analysis should assist in attribution efforts.
- **Honey Pot/Honey Net.** Organizations should have a mirror network to entice attackers to target first, whereby defenders can monitor offensive tactics, techniques, and procedures and apply defensive strategies to the organizations' true networks. In 2013 a Trend Micro researcher created a fake water utility supervisory control and data acquisition system and observed suspected Chinese espionage agents, known as "Comment Crew," gain access to the "honeypot" via an infected MS Word document, and monitored their movements about the system.[27]
- **Active Defense Tools.** Examples of such tools include those capable of opening trigger ports on hosts, whereby attackers would automatically get identified and blacklisted. Other tools include those able to identify the real IP address of a web user, even one behind a proxy; and those that employ geo-location and a browser's share function to pinpoint the physical location of a web user. Last, there are also tools capable of detecting network-reconnaissance and of feeding attackers phony information using networks of virtualized decoys.[28]
- **Denial and Deception.** These include techniques used to mislead attackers through technical solutions. Some examples are the implementation of an operating system that recognizes when an attacker is downloading a rootkit for installation, and deletes it without notifying the attacker. Another is the creation of a website that provides files of data compiled at random from real files to confuse attackers into seeing nonexistent connections. File transfer utilities that identify common attack signatures, and pretend to succumb by responding in the same way an affected system would are useful as well. [29]

Conclusion

Active cyber defense can-not curb most malicious activity in cyberspace. Too many variables make it ineffective and potentially

[27] Juha Saarinen, "Chinese Hackers Take Over Fake Water Utility," *ITNews*, August 5, 2013.

[28] Kelly Jackson Higgins, "Free Active Defense Tools Emerge," *Dark Reading*, July 11, 2013.

[29] N. Rowe, "Counterplanning Deceptions to Foil Cyber-Attack Plans," in *Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society* (West Point: IEEE, 2003),203-211; N. Rowe and H. Rothstein, "Two Taxonomies of Deception for Attacks on Information Systems," *Journal of Information Warfare* 3, no. 2 (2004): 27-39.

catastrophic. Attacks have to be destructive to communicate displeasure to the aggressor while ensuring commensurate damage is inflicted. Therein lies the crux of the problem: being able to identify, execute, and control a measured destructive response in a timely manner. Cyberspace is fraught with examples of actor missteps and malware that has escaped to cause unintended harm to third-party systems. While fortunately cyber conflicts have not yet escalated into greater military engagements, this may change as nefarious activity continues without diplomatic, economic, military repercussion or consequence. There is little empirical evidence on which to base informed judgments concerning cyber strategies, which in turn increases the risk of unintended consequences. Moreover, developing offensive cyber capabilities does not preclude adversaries from constructing similar capabilities. Until a better understanding of how cyberpower can be leveraged as a means of détente, it is more prudent to increase efforts in building cyber defenses, while maintaining open dialogues with states to bridge gaps in understanding and language. In this case, the idea the best defense is a good offense should be viewed as a last resort, and not as a first choice.