GEORGETOWN UNIVERSITY PRESS

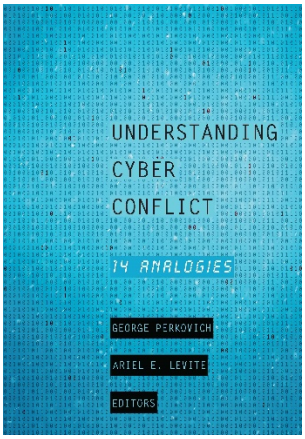
Active Cyber Defense: Applying Air Defense to the Cyber Domain

Dorothy E. Denning and Bradley J. Strawser

From *Understanding Cyber Conflict: Fourteen Analogies*

George Perkovich and Ariel E. Levite, Editors

Published by Georgetown University Press



For additional information about the book:

http://press.georgetown.edu/book/georgetown/understanding-cyber-conflict

12 Active Cyber Defense

APPLYING AIR DEFENSE TO THE CYBER DOMAIN

DOROTHY E. DENNING AND BRADLEY J. STRAWSER

In the domain of cyber defense, the concept of active defense is often taken to mean aggressive actions against the source of an attack. It is given such names as "attack back" and "hack back" and is equated to offensive cyber strikes. It is considered dangerous and potentially harmful, in part because the apparent source of an attack may be an innocent party whose computer has been compromised and exploited by the attacker; so hacking back could be reckless and unfair.

But active cyber defense is a much richer concept. When properly understood, it is neither offensive nor necessarily dangerous. Our approach is to draw on concepts and examples from air defense to define and analyze cyber defenses. We show that many common cyber defenses—such as intrusion prevention—have active elements, and we examine two case studies that employed active defenses effectively and without harming innocent parties. We examine the ethics of active cyber defenses along four dimensions: scope of effects, degree of cooperation, types of effects, and degree of automation. Throughout, we use analogies from air defense to shed light on the nature of cyber defense and to demonstrate that active cyber defense is properly understood as a legitimate form of defense that can be executed according to well-established ethical principles.

Other authors have ably addressed the ethics of active defense. D. Dittrich and K. E. Himma, for example, contributed substantially to initial thinking in this area.[1] This chapter seeks to advance analysis by applying air defense principles to the cyber domain and by exploring the moral and strategic issues raised by active cyber defense.

Defining Active and Passive Cyber Defense

Because our definitions of active and passive cyber defense are derived from those for air defense, we begin by reviewing active and passive air and missile defense.

Active and Passive Air and Missile Defense

For the United States, Joint Publication 3-01, *Countering Air and Missile Threats*, defines *active air and missile defense* (AMD) as a "direct defensive action taken to

destroy, nullify, or reduce the effectiveness of air and missile threats against friendly forces and assets." The definition goes on to say that active AMD "includes the use of aircraft, AD [air defense] weapons, missile defense weapons, electronic warfare (EW), multiple sensors, and other available weapons/capabilities."[2] Active AMD describes such actions as shooting down or diverting incoming missiles and jamming hostile radar or communications.

The Patriot surface-to-air missile system is an example of an active defense system. It uses an advanced aerial-interceptor missile and high-performance radar system to detect and shoot down hostile aircraft and tactical ballistic missiles.[3] Patriots were first deployed in Operation Desert Storm in 1991 to counter Iraqi Scud missiles. Israel's Iron Dome anti-rocket interceptor system has a similar objective of defending against incoming air threats. According to reports, the system intercepted more than three hundred rockets that Hamas fired from Gaza into Israel during the November 2012 conflict, with a success rate of 80 to 90 percent.[4] At the time, Israel was also under cyber assault, and Prime Minister Benjamin Netanyahu said the country needed to develop a cyber defense system similar to Iron Dome.[5]

Another example of an active air defense system is the United States' Operation Noble Eagle.[6] Launched the morning of September 11, 2001, minutes after terrorists hijacked the first aircraft, the operation has become a major element of homeland air defense, which includes combat air patrols, air cover support for special events, and sorties in response to possible air threats. Noble Eagle pilots can potentially shoot down hostile aircraft, although so far none have done so. However, over the years, they have intercepted and escorted numerous planes to airfields.

In contrast to active defense, *passive air and missile defense* is defined as "all measures, other than active AMD, taken to minimize the effectiveness of hostile air and missile threats against friendly forces and assets . . . [noting that] these measures include detection, warning, camouflage, concealment, deception, dispersion, and the use of protective construction. Passive AMD improves survivability by reducing the likelihood of detection and targeting of friendly assets and thereby minimizing the potential effects of adversary reconnaissance, surveillance, and attack."[7] Passive AMD includes such actions as concealing aircraft with stealth technology. It also covers monitoring the airspace for adversary aircraft and missiles but not actions that destroy or divert them.

Active and Passive Cyber Defense

We adapt the definitions of active and passive air defense to the cyber domain by replacing the term "air and missile" with "cyber." This gives us the basic definitions: *active cyber defense* is a direct defensive action taken to destroy, nullify, or reduce the effectiveness of cyber threats against friendly forces and assets, and *passive cyber defense* is all measures, other than active cyber defense, taken to minimize the effectiveness of cyber threats against friendly forces and assets. Put another way, active defenses are direct actions taken against specific threats,

while passive defenses focus more on protecting cyber assets from a variety of possible threats.

Using these definitions, we now examine various cyber defenses to see whether they are active or passive. We begin with encryption, which is clearly a passive defense. It is designed to ensure that information is effectively inaccessible to adversaries that intercept encrypted communications or download encrypted files, but it takes no action to prevent such interceptions or downloads. Steganography is similarly passive. By hiding the very existence of information within a cover such as a photo, it serves as a form of camouflage in the cyber domain. Other passive defenses include security engineering; configuration monitoring and management; vulnerability assessment and mitigation; application whitelisting (to prevent unauthorized programs from running); limits on administrator access; logging, backup, and recovery of lost data; and education and training of users. None of these involve direct actions against a hostile threat.

User authentication mechanisms can be active or passive. For example, consider a login mechanism based on usernames and passwords that denies access when either the username or password fails to match a registered user. We consider this passive if no further action is taken against an adversary attempting to gain access by this means. Indeed, the person might try again and again, perhaps eventually succeeding. If the mechanism locks the account after three tries, then it has an active element insofar as this particular adversary will be unable to gain entry through that account, at least temporarily. However, it does not stop the adversary from trying other accounts or from trying to gain access through other means such as a malware attack. Nor does it prevent an attacker who stole an account and password from gaining access to the system.

Now consider the Defense Advanced Research Project Agency's Active Authentication program, which seeks to validate users continuously using a wide range of physical and behavioral biometrics such as mouse and typing patterns and how messages and documents are crafted.[8] If at any time a user's actions are inconsistent with their normal biometric patterns (called their cognitive fingerprint), access could be terminated. Such a mechanism would be more active than the password mechanism, as it could keep the adversary from entering and then exploiting any legitimate account on the system. It might even thwart a malware attack, as the malware's behavior would not match that of the account under which it is running.

Consider next a simple firewall access control list (ACL) that blocks all incoming packets to a particular port on the grounds that because the system does not support any services on that port, it would be an open door for attackers. We consider this passive, as it serves more to eliminate a vulnerability than to address a particular threat. However, the ACL would become an element of an active defense if an intrusion prevention system detected hostile traffic and then revised the ACL to block the offending traffic. An intrusion detection system alone is considered more passive, as it serves primarily as a means of detection and warning.

Anti-malware (or antivirus) tools have much in common with intrusion prevention systems. They detect malicious software, including viruses, worms, and Trojans, and then (optionally) block the code from entering or executing on a protected system. Typically these tools are regularly updated to include signatures for new forms and variants of malware that are detected across the Internet. In this sense, the active defenses are applied globally over the Internet. After new malware is discovered, security vendors create and distribute new signatures to the customers of their anti-malware products.

Intrusion prevention can likewise be performed on a broader scale than a single network or even an enterprise. For example, the Internet protocol (IP) addresses of machines that are spewing hostile packets can be shared widely through blacklists and then blocked by Internet service providers. Indeed, victims of massive denial of service attacks frequently ask upstream service providers to drop packets coming from the originating IP addresses.

Anti-malware and intrusion prevention systems can be integrated to form powerful active defenses. In many respects, the combined defenses would resemble an active air and missile defense system that detects hostile air threats and takes such actions as shooting them down or jamming their communications, except that in cyberspace the defenses are applied to hostile cyber threats such as malicious packets and malware. Rather than targeting incoming ballistic missiles, cyber defenses take their aim at packets that act like cyber missiles.

Honeypots, which lure or deflect attackers into isolated systems where they can be monitored, are another form of active defense. They are similar to the decoys used in air defense that deflect missiles from their intended targets.

In addition to playing a role in network security, active cyber defenses have been used to take down botnets (networks of compromised computers) and counter other cyber threats. The following two examples illustrate.

Coreflood Takedown

In April 2011 the Federal Bureau of Investigation (FBI), Department of Justice, and the nonprofit Internet Systems Consortium (ISC) deployed active defenses to take down the seven-year-old Coreflood botnet.[9] At the time, the botnet comprised over two million infected computers, all under the helm of a set of command-and-control (C2) servers. The bot malware installed on the machines was used to harvest usernames and passwords, as well as financial information to steal funds. One C2 server alone held about 190 gigabytes of data stolen from more than 400,000 victims.

The active defense included several steps. First, the US District Court of Connecticut issued a temporary restraining order that allowed ISC to swap out Coreflood's C2 servers for its own servers. The order also allowed the government to take over domain names used by the botnet. When the infected machines reached out to the new C2 servers for instructions, the bots were commanded to stop. The malware reactivated following a reboot, but each time it contacted a C2 server, it was instructed to stop. The effect was to neutralize, but not eliminate, the malware installed on the compromised machines. To help victims remove

the malware, the FBI provided the IP addresses of infected machines to Internet service providers (ISPs) so they could notify their customers. In addition, Microsoft issued an update to its Malicious Software Removal Tool so victims could get rid of the code.

Using the air defense analogy, the Coreflood takedown can be likened to an active defense against hijacked aircraft, where the hijackers were acting on instructions transmitted from a C2 center. In this situation, the air defense might jam the signals sent from the center and replace them with signals that command the hijackers to land at specified airports. The airports would also be given information to identify the hijacked planes so that when they landed, the hijackers could be removed.

This approach of neutralizing the damaging effects of botnets by commandeering their C2 servers has been used in several other cases. Microsoft, for example, received a court order in November 2012 to continue its control of the C2 servers for two Zeus botnets. Because Zeus had been widely used to raid bank accounts, the operation has no doubt prevented considerable harm.[10]

Georgian Outing of Russia-Based Hacker

In October 2012 Network World reported that the Georgian government had posted photos of a Russia-based hacker who had waged a persistent, months-long campaign to steal confidential information from Georgian government ministries, Parliament, banks, and nongovernmental organizations.[11] The photos, taken by the hacker's own webcam, came after a lengthy investigation that began in March 2011 when a file on a government computer was flagged by an antivirus program. After looking into the incident, government officials determined that three hundred to four hundred computers in key government agencies had been infected with the malware and that they had acquired it by visiting infected Georgian news sites that had pages with headlines such as "NATO Delegation Visit in Georgia" and "US-Georgian Agreements and Meetings." Once installed, the malware searched for documents using keywords such as "USA," "Russia," "NATO," and "CIA" and then transmitted the documents to a drop server where the spy could retrieve them.

Georgia's initial response included blocking connections to the drop server and removing the malware from the infected websites and personal computers. However, the spy did not give up and began sending the malware out as a portable document format file attachment in a deceptive email allegedly from admin@president.gov.ge.

The Georgian government then let the hacker infect one of its computers on purpose. On that computer, it hid its own spying program in a .ZIP archive titled "Georgian-NATO Agreement." The hacker took the bait, downloaded the archive, and unwittingly launched the government's code. The spyware turned on the hacker's webcam and began sending images to the government. It also mined the hacker's computers for documents, finding one that contained instructions in Russian from the hacker's handler about whom to target and how, as well as circumstantial evidence suggesting the Russian government's involvement.

Again, using the air defense analogy, the steps taken to block the exfiltration of files from compromised computers to the drop servers could be likened to jamming the transmission of sensitive data acquired with a stolen reconnaissance plane to the thieves' drop center. The steps taken to bait the hacker into unwittingly stealing and installing spyware might be likened to a command intentionally permitting the theft of a rigged reconnaissance plane with hidden surveillance equipment that sends the data it collects about the thieves back to the command.

Characteristics and Ethical Issues in Active Cyber Defense

In this section, we offer a set of distinctions for characterizing the different types of active defense described in the preceding section and discuss some of the ethical issues raised by each.

Scope of Effects

The first set of distinctions pertains to the scope of effects of an active defense. An active defense is said to be internal if the effects are limited to an organization's own internal network. If it affects outside networks, it is said to be external.

Drawing on the air defense analogy, an internal cyber defense is similar to an air defense system that takes actions against an incoming missile or hostile aircraft after it has entered a country's airspace, while an external cyber defense is similar to an air defense system that operates in someone else's airspace or attacks the base in a foreign country where the missile is being launched or the hostile aircraft is departing. Antiballistic missile defenses that operate against warheads during their boost phase are generally external, taking place in hostile territory, while those that operate during the terminal phase are likely to be internal.

We consider defenses that involve sharing threat information with outside parties to be external. An example is the Enhanced Security Services (ECS) program operated by the Department of Homeland Security (DHS). Under the program, DHS shares with commercial service providers indicators of cyber threats. The providers, in turn, use this information to better protect their customers.[12] Defenses that involve collecting intelligence from outside sources—say, by installing early warning sensors on their networks—are also considered external. Most of the effects in the Coreflood takedown were external. The C2 servers themselves were external, and when ISC took them over, they instructed bots in outside networks to stop. In contrast, most of the effects in the Georgian case were internal. Connections to the drop server were blocked on internal networks, and internal machines were cleaned of the malware. However, the case also had external effects—for example, the infection of the hacker's own computer with spyware.

Ethical Issues

In general, most of the ethical issues regarding active defenses concern external active defenses. They are discussed in the next section when we distinguish

cooperative external defenses from noncooperative ones. However, even internal defenses can raise ethical issues. For example, inside users might complain that their rights to free speech were violated if internal defenses blocked their communications with outside parties. In addition, internal defenses do nothing to mitigate threats across cyberspace. By not even sharing threat information with outsiders, internal defenses expose external networks to continued harm that might be avoided if the defenses were applied to them as well. Arguably, at least in terms of national cyber defense, a better moral choice would be to help mitigate cyber threats more broadly. As discussed in the next section, the federal government has taken several steps to promote sharing of threat data, including the ECS program.

Returning to the air defense analogy, a missile defense system that only shot down missiles headed to military bases would not be as "just" as one that also shot down missiles headed to civilian targets such as cities and malls. However, it would be unreasonable to expect that missile defense system to protect the airspace of other countries, at least absent an agreement to do so.

Degree of Cooperation

The second set of distinctions pertains to the degree of cooperation in an active defense. If all effects against a particular network are performed with the knowledge and consent of the network owner, they are said to be cooperative. Otherwise, they are classified as noncooperative. For this discussion, we assume that network owners are authorized to conduct most defensive operations on their own networks, at least as long as they do not violate any laws or contractual agreements with their customers or users. Thus, the distinction applies mainly to active defenses with external effects.

Using the air defense analogy, a cooperative cyber defense is similar to an air defense system that shoots down missiles or hostile aircraft in the airspace of an ally that has requested help, and a noncooperative cyber defense is akin to an air defense system that shoots them down in the adversary's own airspace.

Antiviral tools are cooperative defenses. Security vendors distribute new signatures to their customers, but the signatures are installed only with the customers' permission. Similarly, sharing blacklists of hostile IP addresses is cooperative. In general, any active defense that does nothing more than share threat information is cooperative.

Defenses become noncooperative when they involve actions taken against external computers without the permission of the user or network owner. In the case of Coreflood, the actions taken against the individual bots were noncooperative. Neither the users of those machines nor the owners of the networks on which they resided agreed to have the bot code stopped. But neither had they agreed to the initial malware infection and subsequent theft of their data. Arguably, any user would prefer that the malware be stopped than be allowed to continue its harmful actions. Further, even though the action was noncooperative, it was deployed under legal authorities, enabled in part by the temporary restraining order. Moreover, the actual elimination of the malware

from the infected machines was a cooperative action involving the machine owners.

Noncooperative defenses include what is sometimes called an attack back, a hack back, or a counterstrike. This defense uses hacking or exploit tools directly against the source of an attack or gets the attacker to unwittingly install software, say, by planting it in a decoy file on a computer the attacker has compromised. The goal might be to collect information about the source of the attack, to block attack packets, or to neutralize the source. Noncooperative defenses also include court-ordered seizures of computers.

Although the Coreflood takedown did not include any sort of hack back, the Georgian case did. In particular, the actions taken to plant spyware on the hacker's computer constituted a noncooperative counterstrike. However, one could argue that the hacker would never have acquired the spyware had he not knowingly and willfully first infected the computer hosting it and, second, downloaded the .ZIP archive containing it. Thus, he was at least complicit in his own infection and ultimate outing.

Ethical Issues

As a rule, noncooperative defenses, particularly those involving some sort of hack back, raise more ethical and legal issues than cooperative ones. In part, this is because most cyber attacks are launched through machines that themselves have been attacked, making it hard to know whether the immediate source of an attack is itself a victim rather than the actual source of malice. They may be hacked servers or bots on a botnet. Thus, any actions taken against the computers could harm parties who are not directly responsible for the attacks. In addition, cyber attacks in general violate computer crime statutes, at least when conducted by private sector entities.

While the argument can be made that some hack backs should be permissible under the law, not everyone agrees, and the topic has been hotly debated.[13] The Department of Justice has advised victims to refrain from any "attempt to access, damage, or impair another system that may appear to be involved in the intrusion or attack." The advice contends that "doing so is likely illegal, under U.S. and some foreign laws, and could result in civil and/or criminal liability."[14] However, government entities—in particular, the military, law enforcement, and intelligence agencies—have or can acquire the authorities needed to perform actions that might be characterized as hacking under certain prescribed conditions.

One might argue that if the government cannot or will not defend private organizations from cyber attacks, then these organizations should be able to come to their own defense even if that includes hacking back. The problem with this argument is that cyber attacks can be stopped without invading the attacker's system—for example, by blocking packets, by removing malware, and by fixing vulnerabilities. For purely defensive purposes, hacking back is not usually necessary. While the primary benefit of hacking back is to identify the attackers and then possibly prosecute or neutralize them, there are well-established ethi-

cal reasons for leaving these actions in the hands of governments and avoiding vigilantism.

If we assume that noncooperative defenses are conducted by or jointly with government entities with the necessary legal authorities, then the primary concern is that innocent parties may be harmed. Then we can draw on the long tradition of just war theory to determine the conditions under which active cyber defenses that pose risks to noncombatants can be ethically justified.

Most just war theorists hold that noncombatant immunity is a key lynchpin to all our moral thinking in war.[15] Thus, noncombatants are never to be intentionally targeted for harm as any part of a justified military action. Traditional just war theory does hold, however, that some actions that will foreseeably but unintentionally harm noncombatants may be permissible so long as that harm is truly unintentional, is proportionate to the good goal achieved by the act, and is not the means itself to achieve the good goal. Grouped together, these principles are known as the doctrine of double effect. The doctrine has come under heavy scholarly debate, with many critics doubting that its principles can hold true for all cases.[16] Meanwhile, others have argued that some revised or narrowed version of the doctrine can still be defended and applied to war.[17] We cannot engage this larger debate here, but we assume that at least some narrow version of the doctrine of double effect is applicable and, as such, is critical for our moral conclusions regarding harm to noncombatants from active cyber defense.

Whether noncombatants' property can be targeted is another matter. Generally, noncombatant property is similarly considered immune from direct and intentional harm since harming a person's property also harms that person. However, as with physical harm, unintended harm of noncombatant property can be permissible in some instances. Moreover, traditional just war theory and the laws of armed conflict can allow for some level of intentional harm to civilian property if it is necessary to block a particularly severe enemy military action and the civilians in question are later compensated. Thus, the ethical restrictions on harm to civilian property are far less strict than for physical harm to civilian persons. This is true for unintentional harms of both kinds and can even allow for some intentional harm to property when necessary if the stakes are high enough and recompense can be made.

In the case of active air defense, systems like Iron Dome are not without risk to civilians. If they happen to be under an incoming rocket's flight path when it is hit, they could be harmed by fallout from the explosion. However, Israel has limited its counterstrikes primarily to rockets aimed at densely populated urban areas. In that situation, any fallout is likely to be substantially less harmful than the effects produced by the rockets themselves if they are allowed to strike. We argue that such a risk imposition can be morally warranted. Note, however, that if Iron Dome created large amounts of dangerous and lethal fallout disproportionate to the lives saved, then its use would not be permissible.

In general, if an air defense system distributes some small risk of harm to civilians under an incoming missile's flight path to protect a much larger number of civilians from even greater harm, then the present conditions make such

defense morally permissible. This is precisely what we find in the case of real-world air defense systems such as Iron Dome. Further, whether the risk of harm is imposed on noncombatants from one's own state or another state is irrelevant. What matters are the moral rights of all noncombatants, including, of course, noncombatants on any side of a given conflict. The point is to minimize collateral harm to all noncombatants.

The same principles should apply to active cyber defense; that is, it should be morally permissible for a state to take an action against a cyber threat if the unjust harm prevented exceeds and is proportionate to any foreseen harm imposed on noncombatants. Indeed, in the cyber domain meeting this demand will often be easy because it is frequently possible to effectively shoot down the cyber missiles without causing any fallout whatsoever. Instead, packets are simply deleted or diverted to a log file. Nobody is harmed.

In some cases, however, an active defense could have a negative impact on innocent parties. To illustrate, suppose that an action to shut down the source of an attack has the effect of shutting down an innocent person's computer that had been compromised and used to facilitate the attack. In this case, the action might still be morally permissible for two reasons. First, the harm induced might be temporary in nature, affecting the computer for a short time until the attack is contained. Second, the harm itself might be relatively minor, affecting only the noncombatant's property and not his or her person. While such effects could possibly further impede other rights of noncombatants, such as their ability to communicate or engage in activity vital to their livelihoods, all these further harms would be temporary in nature and could even be compensated for, if appropriate, after the fact. This is not to disregard the rights of noncombatants and use of their property for furthering other rights in our moral calculus but simply recognizes that different kinds and severities of harm result in different moral permissions and restrictions.

That the harm itself is likely to be nonphysical is quite significant in our moral reasoning conclusions for active cyber defense. If it is permissible in some cases to impose the risk of physical harm on noncombatants as part of a necessary and proportionate defensive action against an incoming missile (as we argued that it could be in the air defense case), then surely there will be cases where it can be permissible to impose the risk of temporary harm to the property of noncombatants to defend against an unjust cyber attack. The point here with active cyber defense is the kind of harms that would be potentially imposed on noncombatants, in general, is the kind of reduced harms that should make such defensive actions permissible.

A caveat, however, is in order. Computers today are used for life-critical functions, such as controlling life support systems in hospitals and operating critical infrastructure such as power grids. In a worst-case scenario, an active defense that affects such a system might lead to death or significant suffering. These risks need to be considered when weighing the ethics of any noncooperative action that could affect noncombatants. In general, defensive actions that do not disrupt legitimate functions are morally preferable over those that do. If the

scope of possible effects cannot be reasonably estimated or foreseen, then the action may not be permissible.

In the case of Coreflood, the takedown affected many noncombatant computers; however, the effect was simply to stop the bot code from running. No other functions were affected, and the infected computer continued to operate normally. Thus, the operation ran virtually no risk of causing any harm whatsoever, let alone serious harm. In the Georgian case, the only harm was to the attacker's own computer, and he brought it on himself by downloading the bait files, thus making himself liable to intentional defensive harm.

Although the discussion here has focused on noncooperative defenses, it is worth noting that while cooperative defenses generally raise fewer issues, they are not beyond reproach. For example, suppose that a consortium of network owners agrees to block traffic from an IP address that is the source of legitimate traffic as well as the hostile traffic they wish to stop. Depending on circumstances, a better moral choice might be to block only the hostile traffic or to work with the owner of the offending IP address to take remedial action.

Types of Effects

The third set of distinctions pertains to the effects produced. An active defense is called sharing if the effects are to distribute threat information—such as hostile IP addresses or domain names or signatures for malicious packets or software—to other parties. Sharing took place in the Coreflood takedown when the FBI provided the IP addresses of compromised machines in the United States to their US ISPs and to foreign law enforcement agencies when the machines were located outside the United States. Another example of sharing is DHS's aforementioned ECS program.

An active defense is called collecting if it takes actions to acquire more information about the threat, for example, by activating or deploying additional sensors or by serving a court order or subpoena against either the source or an ISP that is likely to have relevant information. In the Coreflood takedown, the replaced C2 servers were set up to collect the IP addresses of the bots so that eventually their owners could be notified. The servers did not, however, acquire the contents of the victims' computers. In the Georgian case, spyware was used to activate a webcam and collect information from the attacker's computer.

An active defense is called blocking if the effects are to deny activity deemed hostile—for example, the traffic from a particular IP address or the execution of a particular program. The Coreflood takedown had the effect of breaking the communications channel from the persons who had been operating the botnet to the C2 servers controlling it. As a result, they could no longer send commands to the bots or download stolen data from the servers. In the Georgian case, connections to the drop servers were blocked to prevent further exfiltration of sensitive data.

Finally, an active defense is called preemptive if the effects are to neutralize or eliminate a source used in the attacks. It can be done, for example, by seizing the computer of a person initiating the attacks or by taking down the C2 servers

for a botnet. In the Coreflood takedown, the hostile C2 servers were put out of commission and the bots neutralized. With further action on the part of the victims, the malware could also be removed.

Using the air defense analogy, the cyber defense of sharing is similar to a missile defense system that reports new missile threats to allies so that they can shoot them down. The cyber defense of collecting is comparable to a missile defense system that installs or activates additional radars or other sensors in response to an increased threat level or that sends out sorties to investigate suspicious aircraft. The cyber defense of blocking is akin to a missile defense system that shoots down incoming missiles or jams their radars and seekers. Finally, the cyber defense of preemption is similar to launching an offensive strike against the air or ground platform launching the missiles.

Some authors regard retaliation or retribution as a form of active defense. However, we consider these operations to be offensive in nature, as they serve primarily to harm the source of a past attack rather than mitigate, stop, or preempt a current one.

Ethical Issues

All four types of cyber operations raise ethical issues. The act of sharing raises issues of privacy and security, particularly if any sensitive information is shared along with the threat information—for example, secret or personal data stolen by an attacker or embedded within the attack traffic. The act of collecting also raises issues about privacy and security, but in this case they relate to the new information that is acquired rather than the dissemination of existing information. One might conclude from this discussion that it is better not to share, but there are equally compelling ethical reasons for sharing threat information. By informing other victims, or potential victims, they can effectively respond to or prevent cyber attacks, and by contacting law enforcement personnel, they can investigate and prosecute those responsible for the attack, thereby preventing further attacks. This ethical dilemma has led to approaches that promote sharing while minimizing the security and privacy risks—for example, by removing sensitive and personally identifiable data.

The US government has taken several steps to encourage the sharing of threat information. With its ECS program, for instance, the government supplies known threat information to the private sector. In early 2015 President Obama issued an executive order promoting the formation of private sector information-sharing and analysis organizations for information exchange and collaboration within the private sector and with the federal government.[18] Then, at the end of the year, Congress passed legislation designed to encourage businesses to share cyber threat information with the government. Although the law requires the removal of personally identifiable information, civil liberties groups were not satisfied with the privacy provisions.[19] The Department of Justice has advised organizations that have been hit by a cyber attack to notify other potential victims, law enforcement, and the Department of Homeland Security.[20] DHS, in turn, may share this information with other potential victims (e.g., through the

ECS program) and provide the notifying organization with additional information and assistance in mitigating the attack.

The act of collecting could also lead to harm if, for example, the sensors and other tools used to collect data on a network have or introduce backdoors or vulnerabilities that other parties could exploit. Even the installation of these tools could cause harm if, in the process, other components of the network are broken. An attempt to install surveillance code in a core router of Syria's main service provider may have taken down Syria's Internet in 2012.[21]

The act of blocking communications raises ethical issues relating to free speech, loss of commerce, and over-blocking. In a worst-case scenario, traffic might be blocked that is important for operating a life support system or critical infrastructure such as power generation and distribution. Likewise, the act of preemption raises ethical issues relating to disabling software or systems. Again, in a worst-case scenario, shutting down a life support system could cause serious harm. Any possible damage would need to be considered when applying any noncooperative cyber defense as discussed in the previous section. Concern over harm should drive technical and policy efforts to limit the effects of defenses, say, by disabling only traffic and software involved in an attack rather than shutting down all traffic and complete systems.

In the Coreflood takedown, it is important to note that the government did not attempt to remove the bot code from infected machines. It only neutralized it by issuing the stop command. Part of its reason for not removing the code was a concern for unanticipated side effects that might damage an infected computer.

Because active cyber defense should not be misconstrued as a form of offense, it is worth explaining why the distinction between offensive retaliation versus legitimate defensive action is so crucial in the ethical dimensions of killing and war. Defensive harm has the lowest ethical barrier to overcome among all possible justifiable harms. That is, if one is being wrongly attacked, then the moral restrictions against using force of some kind to block that wrongful attack are (relatively) few. All people have a right not to be harmed unjustly. If one side is attempting to harm another unjustly, then the former has made itself morally liable to suffer defensive harm as part of an act taken to thwart its unjust act. The side being wrongly attacked may permissibly harm its attacker to block or thwart the attack against it so long as the defensive action meets two criteria. First, inflicting the defensive harm must be necessary to block the unjust attack. If the defensive harm in question does nothing to block the liable party's unjust attack, then it is retributive punishment, or something else, but not properly an act of defense. Second, the defensive harm must be proportionate to the unjust harm to be blocked. If a foreign plane was found conducting reconnaissance over a state's territory without permission during peacetime, then the foreign state may have made itself liable to some form of defensive action such as being escorted to an airfield. However, it would be disproportionate and wrong to shoot the plane down or, even worse, to shoot down commercial planes flying under the foreign state's flag.

In general, there must be some reasonable correlation and proper "fit" between the extent of defensive response and the degree of liability of the offending party.[22] In the case of an active cyber defense, if the act is truly a defensive effort to block an unjust attack, then so long as it is necessary and proportionate, it will usually be ethically permissible. In the Georgian case, the government responded to the cyber espionage operation against it with its own espionage operation against the hacker. It did not destroy software and data on the hacker's computer.

Degree of Automation

The final set of distinctions pertains to the degree of human involvement. An active defense is said to be automatic if no human intervention is required and to be manual if key steps require the affirmative action of humans.

Most anti-malware and intrusion prevention systems have both manual and automated components. Humans determine what goes into the signature database, and they install and configure the security software, including a range of response actions. However, the processes of signature distribution, malicious code and packet detection, and initial response are automated.

In the Coreflood takedown, the execution of the stop commands was fully automated through the C2 servers. However, humans played an important role in the operational planning and decision-making, the analysis of the botnet code and the effects of issuing a stop command, the acquisition of the restraining order, and the swapping out of the C2 servers. Thus, the entire operation had both manual and automatic aspects. In the Georgian case, much of the investigation involved manual work, including analyzing the code, determining what the hacker was looking for, and setting up the bait with the spyware. But the key element in the outing—namely, the operation of the spyware—was automated. Once the hacker downloaded the .ZIP archive, the program did the rest.

Applying once again the air defense analogy, an automatic cyber defense is similar to a missile defense system that automatically shoots down anything meeting the preset criteria for being a hostile aircraft or incoming missile, whereas a manual cyber defense would act as Operation Noble Eagle, where humans play a critical role both in recognizing and responding to suspicious activity in US airspace.

Ethical Issues

In general, on the one hand, manual actions give humans a greater opportunity to contextualize their ethical decisions. Rather than configuring a system to always respond in a certain way, humans can take into account the source or likely source of a perceived threat, its nature, the broader circumstances, and the likely consequences of taking certain actions against it. This is vital to Noble Eagle, where most incidents turn out to be nonhostile and lives are at stake. On the other hand, given that manual actions take longer to execute than automated ones, they potentially allow greater damage to incur before the threat is mitigated.

In the cyber domain, where actions can take place instantaneously, automated defenses become critical. That is, the speed of some actions in the cyber domain are such that a cyber defense must be automated to have any effect against the attack. Perhaps for this reason the Defense Department has exempted some cyber actions from its recent "man in the loop" legal requirements for automated weapon systems.[23] If a hostile actor has launched an attack to cause a power generator to explode, then an automated response that successfully blocks the attack without causing unnecessary harm is morally superior to a manual one that comes too late.

However, this does not mean that all cyber defenses should be automated. To argue that all cyber actions should be exempt from the man-in-the-loop requirement would be ethically (and strategically) problematic. The nature of a defense and its potential effects—particularly the potential severity of its foreseeable harms—must be weighed in any decision to automate. The cyber case is unique in that the speed of many cyber attacks necessitates that many defenses be automated to be effective in any way. But if the effects of automating a given defense would lead to too great a risk of impermissible harm, then it should not be done, even if this decision essentially nullifies its efficacy entirely. Thankfully, given the aforementioned reasons regarding the predictable effects that most forms of active cyber defense would produce, we find that in many cases their automation could be permissible.

Conclusions

Using analogies from air defense, active cyber defense is a rich concept that, when properly understood and executed, is neither offensive nor necessarily harmful and dangerous. Rather, it can be executed in accordance with the well-established ethical principles that govern all forms of defense—namely, principles relating to harm, necessity, and proportionality. In many cases, such as with most botnet takedowns, active defenses mitigate substantial harm while imposing little or none of their own.

While active defenses can be morally justified in many cases, we do not mean to imply that they always are. All plausible effects must be considered to determine what, if any, harms can follow. If harms cannot be estimated or are unnecessary or disproportionate to potential benefits gained, an active defense cannot be morally justified.

In considering active defenses, we have assumed that they would be executed under appropriate legal authorities. In particular, they would be conducted by authorized government entities or by private companies operating under judicial orders or otherwise within the law. We leave open the question of how far companies can go in areas where the law is unclear or untested. While such active defenses as sharing attack signatures and hostile IP addresses and domain names have raised few legal questions, an active defense that deleted code or data on the attacker's machine would raise more. No doubt, this area will likely continue to inspire lively discussions and debates.

Notes

The views expressed in this document are those of the authors and do not reflect the official policy or position of the Department of Defense or the US government. An earlier version of this chapter appeared in Emily O. Goldman and John Arquilla, eds., *Cyber Analogies* (Monterey, CA: Naval Postgraduate School, 2014).

1. D. Dittrich and K. E. Himma, "Active Response to Computer Intrusions," in *The Handbook of Information Security*, ed. H. Bidgoli (Somerset, NJ: John Wiley & Sons, 2005).

2. Department of Defense, Joint Publication 3–01, *Countering Air and Missile Threats* (Washington, DC: Department of Defense, March 23, 2012), http://www.dtic.mil/doctrine/new_pubs/jp3_01.pdf.

3. "MIM-104 Patriot," Wikipedia, no date, accessed November 6, 2012, https://en.wikipedia.org/wiki/MIM-104_Patriot.

4. I. Kershner, "Israeli Iron Dome Stops a Rocket with a Rocket," *New York Times*, November 18, 2012, http://www.nytimes.com/2012/11/19/world/middleeast/israeli-iron-dome-stops-a-rocket-with-a-rocket.html?_r=0.

5. G. Ackerman and S. A. Ramadan, "Israel Wages Cyber War with Hamas as Civilians Take up Computers," *Bloomberg,* November 19, 2012, http://www.bloomberg.com/news/2012-11-19/israel-wages-cyber-war-with-hamas-as-civilians-take-up-computers.html.

6. Air Force, Operation Noble Eagle, Air Force Historical Studies Office, posted September 6, 2012, http://www.afhistory.af.mil/FAQs/Fact-Sheets/Article/458956/2001-operation-noble-eagle.

7. Department of Defense, "Countering Air and Missile Threats."

8. A. Keromytis, "Active Authentication," Defense Advanced Research Projects Agency, no date, accessed January 13, 2016, http://www.darpa.mil/program/active-authentication.

9. K. Zetter, "With Court Order, FBI Hijacks 'Coreflood' Botnet, Sends Kill Signal," *Wired*, April 13, 2011, https://www.wired.com/threatlevel/2011/04/coreflood/; K. Zetter, "FBI vs. Coreflood Botnet: Round 1 Goes to the Feds," *Wired*, April 26, 2011, https://www.wired.com/threatlevel/2011/04/coreflood_results/; and K. J. Higgins, "Coreflood Botnet an Attractive Target for Takedown for Many Reasons," *Dark Reading*, April 14, 2011, http://www.darkreading.com/risk/coreflood-botnet-an-attractive-target-for-takedown-for-many-reasons/d/d-id/1135557?.

10. R. Lemos, "Microsoft Can Retain Control of Zeus Botnet under Federal Court Order," eWeek, December 1, 2012, http://www.eweek.com/security/microsoft-can-retain-control-of-zeus-botnet-under-federal-court-order/.

11. J. Kirk, "Irked by Cyberspying, Georgia Outs Russia-Based Hacker—with Photos," *Computerworld*, October 30, 2010, http://www.computerworld.com/article/2493051/cybercrime-hacking/irked-by-cyberspying—georgia-outs-russia-based-hacker——with-photos.html.

12. Department of Homeland Security, "Enhanced Cybersecurity Services (ECS)," October 14, 2015, http://www.dhs.gov/enhanced-cybersecurity-services.

13. D. E. Denning, "The Ethics of Cyber Conflict," in *The Handbook of Information and Computer Ethics*, ed. K. E. Himma and H. T. Tavani (Somerset, NJ: John Wiley & Sons, 2012), 407–28; E. Messmer, "Hitting Back at Cyberattackers: Experts Discuss Pros and Cons," *Network World*, November 1, 2012, http://www.networkworld.com/article/2161144/security/hitting-back-at-cyberattackers—experts-discuss-pros-and-cons.html; and Steptoe, "The

Hackback Debate," Steptoe Cyberblog, November 2, 2012, http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/.

14. Department of Justice, Cybersecurity Unit, "Best Practices for Victim Response and Reporting of Cyber Incidents," April 2015, http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf.

15. M. Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (New York: Basic Books, 1977); T. Nagel, "War and Massacre," *Philosophy and Public Affairs* 1, no. 2 (1972): 123–44; D. Rodin, *War and Self-Defense* (New York: Oxford University Press, 2003); and B. Orend, *The Morality of War* (Peterborough, ON: Broadview Press, 2006).

16. N. Davis, "The Doctrine of Double Effect: Problems of Interpretation," *Pacific Philosophical Quarterly* 65 (1984): 107–23; F. Kamm, "Failures of Just War Theory: Terror, Harm, and Justice," *Ethics* 114 (2004): 650–92; A. McIntyre, "Doing Away with Double Effect," *Ethics* 111 (2001): 219–55; and U. Steinhoff, *On the Ethics of War and Terrorism* (Oxford: Oxford University Press, 2007).

17. J. McMahan, "Revising the Doctrine of Double Effect," *Journal of Applied Philosophy* 11, no. 2 (1994): 201–12; W. S. Quinn, "Actions, Intentions, and Consequences: The Doctrine of Double Effect," *Philosophy and Public Affairs* 18 (1989): 334–51; and D. Nelkin and S. Rickless, "Three Cheers for Double Effect," *Philosophy and Phenomenological Research*, December 2012, http://onlinelibrary.wiley.com/doi/10.1111/phpr.12002/full.

18. Barack Obama, "Executive Order—Promoting Private Sector Cybersecurity Information Sharing," The White House, February 13, 2015, https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

19. E. Chabrow, "Obama Signs Cyberthreat Information Sharing Bill," Gov Info Security, December 18, 2015, http://www.govinfosecurity.com/congress-approves-cyberthreat-information-sharing-bill-a-8762.

20. Department of Justice, Cybersecurity Unit, "Best Practices."

21. J. Bamford, "The Most Wanted Man in the World," *Wired*, August 2014, 2016, http://www.wired.com/2014/08/edward-snowden/.

22. J. McMahan, "The Basis of Moral Liability to Defensive Harm," *Philosophical Issues* 15 (2005): 386–405; and J. Quong, "Liability to Defensive Harm," *Philosophy & Public Affairs* 40, no. 1 (2012): 45–77.

23. Ashton Carter, "Autonomy in Weapon Systems," Department of Defense Directive Number 3000.09, November 21, 2012, www.dtic.mil/whs/directives/corres/pdf/300009p.pdf; and S. Gallagher, "US Cyber-weapons Exempt from 'Human Judgment' Requirement," *Ars Technica*, November 29, 2012, http://arstechnica.com/tech-policy/2012/11/us-cyber-weapons-exempt-from-human-judgment-requirement/.