Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

This is an invited essay by the 2013 IFIP TC-11 Kristian Beckman Award recipient

Framework and principles for active cyber defense☆

*Dorothy E. Denning**

Naval Postgr aduate School, Monterey, USA

ARTICLE INFO

Article history:
Received 28 October 2013
Accepted 10 November 2013

Keywords:
Cyber security
Cyber ethics
Active defense
Hacking back
Air and missile defense

ABSTRACT

This essay offers a broad view of active defense derived from the concept of active air and missile defense. This view admits a range of cyber defenses, many of which are widely deployed and considered essential in today's threat environment. Instead of equating active defense to hacking back, this wider interpretation lends itself to distinguishing different types of active defense and the legal and ethical issues they raise. The essay will review the concepts of active and passive air and missile defenses, apply them to cyberspace, describe a framework for distinguishing different types of active cyber defense, and finally suggest legal and ethical principles for conducting active cyber defense.

1. Introduction

The concept of active cyber defense has raised red flags within the computer security community. Gary McGraw, Chief Technology Officer of Cigital, for example, has called it "irresponsible" and a "recipe for disaster," adding, "The last thing we need in computer security is a bunch of vigilante yoo-hoos and lynch mobs." (McGraw, 2013) His remarks are based largely on a concept of active defense based on "hacking back" or "attacking the attacker," with the possibility of harming innocent persons in the process. Surely, if this is what active defense is all about, then it *should* give us pause.

This essay offers a broader view of active defense derived from the concept of active air and missile defense used by the US Department of Defense. This view admits a range of cyber defenses, many of which are widely deployed and considered essential in today's threat environment. Instead of equating active defense to hacking back, this wider interpretation lends itself to distinguishing different types of active defense and the legal and ethical issues they raise. The essay will review the concepts of active and passive air and missile defenses, apply them to cyberspace, describe a framework for distinguishing different types of active cyber defense, and finally suggest legal and ethical principles for conducting active cyber defense. It draws on work done in collaboration with colleague and ethicist Bradley Strawser in the Defense Analysis Department at the Naval Postgraduate School (Denning and Strawser, 2013).

2. Active and passive air and missile defense

US military doctrine distinguishes between active and passive air defenses. It defines *Active Air and Missile Defense (AMD)* as:

☆ The views expressed in this document are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

* Tel.: +1 831 656 3105.
E-mail address: dedennin@nps.edu.

0167-4048/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2013.11.004

"direct defensive action taken to destroy, nullify, or reduce the effectiveness of air and missile threats against friendly forces and assets." Active AMD is said to include "the use of aircraft, AD [air defense] weapons, missile defense weapons, electronic warfare (EW), multiple sensors, and other available weapons/capabilities" (JP 3-01, 2012). It characterizes such actions as shooting down or diverting incoming missiles and jamming hostile radar or communications.

An example of an active air and missile defense system is the Patriot surface-to-air missile system, which uses an advanced aerial interceptor missile and high performance radar system to detect and shoot down hostile aircraft and tactical ballistic missiles (Patriot, 2012). 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 300 rockets fired by Hamas from Gaza into Israel during the November 2012 conflict, with a success rate of 80–90 percent (Kershner, 2012). At the time, Israel was also under cyber assault, and Prime Minister Benjamin Netanyahu said that the country needed to develop a cyber defense system similar to Iron Dome (Ackerman and Ramadan, 2012).

Another example of an active air defense system is the US's Operation Noble Eagle (Air Force, 2012). Launched minutes after the first aircraft was hijacked the morning of September 11, 2001, the operation has become a major element of homeland air defense through its combat air patrols, air cover support for special events, and sorties in response to possible air threats. Although Noble Eagle pilots can potentially shoot down hostile aircraft, so far none have done so. However, they have intercepted and escorted numerous planes to airfields over the years.

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." (JP 3-01, 2012) It includes such actions as concealing aircraft with stealth technology. It covers monitoring the airspace for adversary aircraft and missiles, but not actions that destroy or divert them.

3. Active and passive cyber defense

The definitions of active and passive air defense can be applied to the cyber domain by replacing the term "air and missile" with "cyber." This gives: *Active Cyber Defense* is direct defensive action taken to destroy, nullify, or reduce the effectiveness of cyber threats against friendly forces and assets. *Passive Cyber Defense* is all measures, other than active cyber defense, taken to minimize the effectiveness of cyber threats against friendly forces and assets. Whereas active defenses are direct actions taken against specific threats, passive defenses focus more on making cyber assets more resilient to attack.

Many popular security controls employ active cyber defenses. Access controls block users from accessing unauthorized files and other resources. Passwords and other user authentication mechanisms block login attempts from adversaries spoofing as legitimate users. Anti-malware systems, intrusion prevention systems (IPSs), and firewalls block malicious software and packets matching threat signatures or exhibiting anomalous behavior. Honeypots lure or deflect attacks into isolated systems where they can be monitored and kept away from production systems. All of these controls are analogous to air and missile defenses that shoot down or deflect incoming missiles and rockets. Active cyber defenses also include operations against systems owned or used by an attacker, including counter-attacks. These are more analogous to air defense operations that attack the air or ground platforms used by the adversary to launch missiles.

Passive cyber defenses include cryptography and steganography (analogous to the use of camouflage and stealth aircraft), security engineering and verification, configuration monitoring and management, vulnerability assessment and mitigation, risk assessment, backup and recovery of lost data, and education and training of users. They also include mechanisms to log and monitor network and host activity (analogous to air monitoring). Intrusion detection systems (IDSs) are essentially passive, but become active when they incorporate elements to abort detected threats, morphing into IPSs.

4. A framework for active cyber defenses

Active cyber defenses can be characterized by four features: scope of effects, degree of cooperation, types of effects, and degree of automation. Together, they place active cyber defenses in a four-dimensional space and provide a framework for distinguishing different types of active cyber defenses and analyzing the ethical issues they raise.

4.1. *Scope of effects*

This feature distinguishes between *internal* defenses, whose effects are limited to the network being defended, and external defenses, whose effects go beyond the network. An internal cyber defense is akin 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 like an air defense system that takes action in someone else's airspace. Most cyber security controls such as access controls and IPSs are internal. An example of an active defense with external effects is a botnet takedown that involves taking over the IP addresses and domain names used for command and control (C2).

4.2. *Degree of cooperation*

This feature distinguishes between active defenses that are *cooperative*, meaning that action is one that is performed against a system with the knowledge and consent of the system owner, from those that are *non-cooperative*, meaning it