The Promise and Peril of Active Cyber Defense

Dr. Irv Lachow

Deputy Director, Cyber Strategy and Execution, MITRE

August 6, 2018

Disclaimer

- ***The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.***

Approved for Public Release; Distribution Unlimited. Case Number 17-2636

Agenda

- *Active Cyber Defense Primer*
- Policy Issues
- References
- ATT&CK
- Discussion

MITRE

Why Is Active Cyber Defense Important?

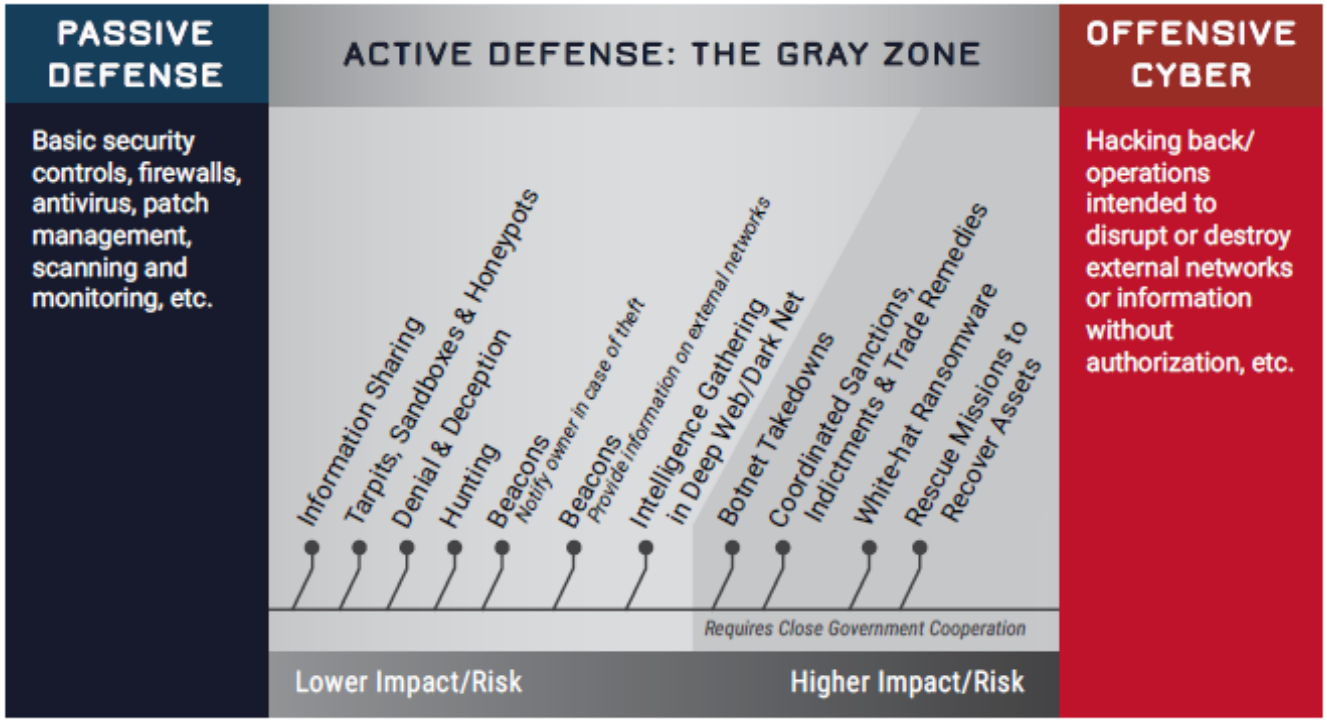
- **Governments alone cannot protect the private sector**
- **Companies are increasingly capable of taking active steps to defend themselves—and are doing so**
- **Current legal and policy guidance is "absent, vague or difficult to operationalize."**
  - Governments are effectively blocking companies from taking action
- **Two most likely outcomes are undesirable:**
  - Companies do nothing
  - Wild West

Approved for Public Release; Distribution Unlimited. Case Number 17-2636

What Does "Active Cyber Defense" Mean?

- **Center for Cyber and Homeland Security**
  - Active defense is a term that captures a spectrum of proactive cybersecurity measures that fall between traditional passive defense and offensive….the term is NOT synonymous with "hacking back." (Emphasis added.)
- **Hoffman and Levite (from Robert Dewar)**
  - An approach to achieving cybersecurity predicated upon the deployment of measures to detect, analyze, identify and mitigate threats…combined with the capability and resources to take proactive or offensive action against threats…
- **DARPA**
  - DARPA's Active Cyber Defense (ACD) program is designed to…[provide] cyber defenders a "home field" advantage: the ability to perform defensive operations that involve direct engagement with sophisticated adversaries in DoD-controlled cyberspace.

Examples of ACD Actions



Source: CCHS

MITRE

Benefits and Risks of ACD Actions

Table 1. **Advantages and Risks of Taking ACD Measures**

ADVANTAGES	RISKS
More advanced knowledge of potential threats and the attacker's capabilities and intent, which helps to mitigate surprise and protect assets	Backfiring due to human error or manipulation by the attacker
Greater range of options to engage the attacker, including flexibility in where, when, and how	Collateral damage as a result of disrupting or damaging an innocent third party computer or network or wrongly attributing the source of an attack
Enhanced ability to disrupt or shut down a planned or ongoing operation even after the initial penetration of the defender's network	Escalation in an exchange between attacker and defender as a result of the attacker's response to ACD measures
Increased likelihood of deterring future attacks by complicating the attack, impeding the use of data, and raising the direct and indirect costs to and risk for the attacker (especially in being identified)	Uncertain strategic implications, including the potential political and legal consequences of measures affecting external networks

Source: Hoffman and Levite

Agenda

- Active Cyber Defense Primer
- *Policy Issues*
- References
- ATT&CK
- Discussion

MITRE

Key Policy and Legal Questions

- Who can do ACD?
- What can they do?
- When can they do ACD?
- Who is help responsible when…?
- How address int'l aspects?
- How address technical developments?

Approved for Public Release; Distribution Unlimited. Case Number 17-2636

Current Legal Frameworks

- **National laws prevent the bulk of ACD activities**
  - Computer Fraud and Abuse Act (CFAA) is most relevant
  - Cybersecurity Act of 2015 allows for the “operation of defensive measures” within certain constraints
- **International Laws**
  - "Formal international treaties have no apparent direct application to the [ACD] questions being considered."
- **Which legal models are most applicable?**
- **This lack of guidance needs to be addressed…**

Source: Lachow, CCHS, Rosenzweig

Congress May Change the Game: An Overview of ACDC Act

- **Provides affirmative defense to criminal prosecution for ACD measures focused on:**
  - Attribution
  - Disruption
  - Monitoring
- **Intention to use ACD measures must be reported to FBI and can be pre-emptively reviewed by them**
- **Caveats:**
  - Cannot “create a threat to public health and safety” or take steps that result in “persistent disruption” of Internet activity
  - For intermediary computers, ACD measures cannot exceed level of activity needed to gather attribution info, nor can they result in intrusive or remote access.

Key Issues Raised Regarding ACDC Act

- **Several key terms are vague**
  - "Persistent," "remote access," "threat to public health or safety"
- **Does not prevent criminal charges for CFAA violations or address civil suits**
- **Does not address ECPA, Wiretap Act, State laws**
- **FBI pre-emptive review may make USG responsible for corporate ACD measures and undermine norms**

Source: Cook

Principles-Based Approach (Market Driven)

- **The Concept**
  - Create normative principles for ACD behaviors
    - Risk-based
    - Formalized via industry-driven code of conduct
  - Use market-based mechanisms to enforce desired behaviors
    - Insurance industry
    - Civil torts
- **Advantages**
  - Relies on incentives to drive behavior
  - Balances risks
  - Adaptable to dynamic environment
- **Challenges**
  - Legal authority is still needed
  - Actions can have global consequences
  - Markets sometimes fail

Source: Hoffman and Levite

MITRE

Government-Licensed Private Security

- **The Concept:**
  - Only authorized firms are allowed to conduct ACD
  - Licensing requirements set by each country
  - Allowed actions would fall short of most aggressive ACD techniques
  - Close cooperation with gov't authorities
- **Advantages**
  - Clear limits about allowable actions
  - Lower risk of collateral damage and escalation
  - Improved public-private cooperation
- **Challenges**
  - Licensing process
  - Oversight process
  - Coordination across nations
  - State-sanctioned activity

Source: Rosenzeig

GWU Task Force "ACD Policy Framework"

- **Fifteen recommended steps for U.S. industry, Executive Branch, and Congress**

- **Key themes**
  - Define range of acceptable actions that balance efficacy and risk
  - Update legal instruments to reflect balanced approach
  - Work towards global standards across nations
  - Strengthen public-private cooperation
  - Create set of best practices that are promulgated across industry

Source: CCHS

UK's Government ACD Program: Overview

- **Goal: "protect the majority of people in the UK from the majority of the harm, caused by the majority of attacks, for the majority of the time."**
- **Led by National Cyber Security Centre**
- **Initial focus on public sector customers**
- **Close public-private cooperation**
- **Program elements**
  - Strengthen infrastructure protocols
  - Secure email
  - Take down criminal websites
  - Filter DNS
  - Strengthen identity authentication

Source: Levy

UK Government ACD Program: Results

- **Takedown service**
  - Removed 121,479 unique phishing sites across 20,763 attack groups hosted in the UK. This reduced median availability of a UK-hosted phishing site from 26 hours to 3 hours.
  - Removed 18,067 unique phishing sites across 2,929 attack groups that were pretending to be UK gov't brand.
- **Secure email**
  - 10% of gov't domains now use Mail Check service
  - Seeing reduction in number of messages spoofed from @gov.uk
- **DNS Filtering**
  - Blocked 134,825 unique DNS queries
  - One in six orgs found security issues to be remedied

Source: Levy

MITRE

Key Takeaways

- Private sector brings key capabilities to the table
- ACD actions need to balance benefits and risks
- Legal clarity is needed
- International aspects may be most challenging
- Government and industry cooperation is essential

MITRE

Agenda

- Active Cyber Defense Primer
- Policy Issues
- *References*
- ATT&CK
- Discussion

MITRE

Key References

- Center for Cyber & Homeland Security (CCHS). *Into the Grey Zone: The Private Sector and Active Defense Against Cyber Threats* (Washington, DC, The George Washington University, 2016).
- Cook, Chris. *Hacking Back in Black: Legal and Policy Concerns with the Updated Active Cyber Defense Certainty Act*, November 20, 2017, https://www.justsecurity.org/47141/hacking-black-legal-policy-concerns-updated-active-cyber-defense-certainty-act/.
- Hoffman, Wyatt and Ariel E. Levite. *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace* (Washington, DC, Carnegie Endowment for International Peace, 2017).
- Lachow, Irving. *Active Cyber Defense: A Framework for Policymakers* (Washington, DC, Center for a New American Security, 2013).
- Levy, Ian. *Active Cyber Defence – One Year On* (London, UK National Cyber Security Centre, 2018).
- Rosenzweig, Paul, Steven P. Bucci and David Inserra. *Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense*, Backgrounder, No 3188 (Washington, DC, The Heritage Foundation, 2017).

Approved for Public Release; Distribution Unlimited. Case Number 17-2636

Agenda

- Active Cyber Defense Primer
- Policy Issues
- References
- *ATT&CK*
- Discussion

Questions?
Comments?
Ideas?

MITRE

ACD Activities Involve Risk Tradeoffs

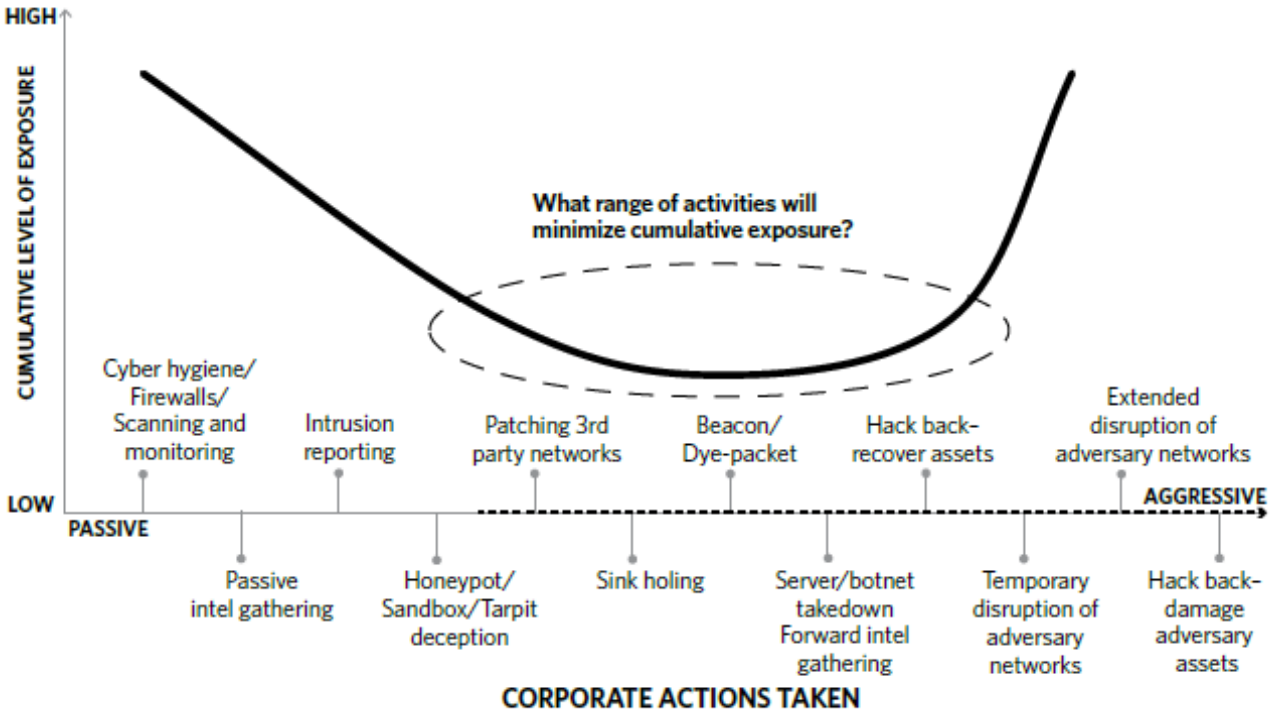
Figure 2. **Balancing Corporate Cyber Risks**

Source: Hoffman and Levite

MITRE

In Theory ACD Risks Can be Quantified

Figure 3. **Cumulative Exposure to Corporations Utilizing ACD**



Source: Hoffman and Levite

MITRE