About the George Washington University Center for Cyber & Homeland Security

The Center for Cyber and Homeland Security (CCHS) at the George Washington University is a nonpartisan “think and do” tank whose mission is to carry out policy-relevant research and analysis on homeland security, counterterrorism, and cybersecurity issues. By convening domestic and international policymakers and practitioners at all levels of government, the private and non-profit sectors, and academia, CCHS develops innovative strategies to address and confront current and future threats.

CCHS was established in early 2015 and integrates the activities and personnel of the Homeland Security Policy Institute (HSPI) and the GW Cybersecurity Initiative.

Download the full report at cchs.gwu.edu

Some rights reserved. Printed in the United States of America.

This report carries a Creative Commons Attribution 4.0 International license, which permits re-use of George Washington University Center for Cyber and Homeland Security’s content when proper attribution is provided. This means you are free to share and adapt Center for Cyber and Homeland Security’s work, or include our content in derivative works, under the following condition: You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

This work is licensed under CC-BY version 4.0 https://creativecommons.org/licenses/by/4.0

© 2016 by Center for Cyber and Homeland Security

Center for Cyber and Homeland Security
2000 Pennsylvania Avenue NW
Washington, DC 20052
www.cchs.gwu.edu
OVER THE PAST SEVERAL DECADES, the private sector in the United States has embraced the computer revolution and the growth of the Internet, and migrated its business activities and operations into an information technology environment. This transition to the online domain has provided tremendous benefits to the private sector, enabling business efficiencies, lowering transaction costs, establishing new products and markets, enhancing internal collaboration, and improving the ability of companies to measure and assess their performance. But as the online domain has developed over the past several decades, new risks have accompanied these benefits; companies have become increasingly vulnerable to the theft of online intellectual property or customer data and the disruption of business operations.

These cyber risks and dependencies have grown in recent years due to the activities of hostile state and non-state actors in cyberspace, who have attacked private sector entities for both political and economic reasons. Companies have enhanced their defenses, and the federal government has placed a higher priority on assisting the private sector, but such measures are not commensurate with the nature of the cyber threat today.

This paper examines a set of capabilities that can help to address this gap, collectively defined under the term active defense:

Active defense is a term that captures a spectrum of proactive cybersecurity measures that fall between traditional passive defense and offense. These activities fall into two general categories, the first covering technical interactions between a defender and an attacker. The second category of active defense includes those operations that enable defenders to collect intelligence on threat actors and indicators on the Internet, as well as other policy tools (e.g. sanctions, indictments, trade remedies) that can modify the behavior of malicious actors. The term active defense is not synonymous with “hacking back” and the two should not be used interchangeably.

The policy discussion on active defense measures in recent years has largely fallen into one of two camps: those who believe that active defense activities are appropriately prohibited under current U.S. law, and those who believe that more active tools should be available to the private sector. What has been missing is a more nuanced discussion of this issue: What measures fall within the scope of active defense, and what are the benefits and risks of each? What measures may be appropriate to use by certain actors, and under what circumstances? What is the role of the federal government in developing a framework and set of norms that can inform such action? And how should policy and law be updated to support private sector active defense in a way that is consistent with both our values and interests, and that can evolve as new technologies are developed?

In other words, how do we move beyond the current policy stalemate of inaction vs. hacking back, and develop appropriate and risk-driven policies for active defense? This paper attempts to go “into the gray zone” and answer these questions. It proposes a normative framework for operationalizing active defense and puts forward a set of policy recommendations that support the implementation of such a framework.

The initial sections of the report provide background and context to this discussion. It begins with a very brief overview of current cyber threats to the private sector, and what is being done by private entities and government agencies to counter these threats. This discussion of the threat is followed by an articulation of U.S. interests in cyberspace and an explanation of the strategic context of active defense, in particular its relation to the issue of cyber deterrence.
The next section of the report provides a historical perspective on the evolution of the term “active defense,” initially in a general national security context and later with respect to cybersecurity. These historical definitions inform the report’s own definition. The report then discusses the upper and lower boundaries of active defense and examines the spectrum of activities that fall within it, including honeypots, beacons, and sinkholing malicious traffic. It makes clear that certain types of high-risk active defense activity by the private sector should be impermissible due to risks of collateral damage and privacy-related concerns, but pushes for greater clarity on whether and how the private sector can utilize lower-risk active defense measures.

Next, the paper provides additional policy context to the issue of active defense, examining the impact of current U.S. laws (e.g., the Computer Fraud and Abuse Act), assessing the policy impact of evolving technologies such as cloud computing and the Internet of Things, and outlining the nascent international framework for active defense.

The final sections of the report lay out the proposed framework for active defense by the private sector. The core of this framework is the spectrum of active defense measures defined earlier in the report, embedded within a broader set of policy, legal, technical, and governance-related considerations, which provide the basis for risk-driven deliberation and decision-making both within companies and between the government and the private sector on active defense. The framework seeks to maximize the effectiveness of the private sector’s ability to defend its most valuable data and assets. It recognizes that a broad suite of technical and non-technical tools is applicable to the countering of cyber threats to the private sector. And it attempts to balance the need to enable private sector active defense measures with other important considerations such as the protection of individual liberties, privacy, and the risks of collateral damage. An additional key aspect of this framework is a risk-driven methodology that can be used to weigh the risks and benefits of action vs. inaction, and to then choose and utilize appropriate tools if and where action is warranted.

This overview of the framework is followed by a detailed discussion of key actors within the framework and what is needed to operationalize it. After this section, the report puts forward a set of near-term policy recommendations for the U.S. executive branch, Congress, and the private sector that are intended to facilitate the implementation and adoption of this framework.

**Actions for the Executive Branch**

1. **The Department of Justice should issue public guidance to the private sector with respect to active defense measures that it interprets to be allowable under current law, indicating that DOJ would not pursue criminal or civil action for such measures assuming that they are related to the security of a company’s own information and systems. Such guidance should be updated on a regular basis consistent with ongoing developments in technology.**

2. **DOJ and the Federal Trade Commission should update their “Antitrust Policy Statement on Cybersecurity Information Sharing” (2014) to state clearly that antitrust laws should not pose a barrier to intra-industry coordination on active defense against cyber threats.**

3. **The Department of Homeland Security should coordinate the development of operational procedures for public-private sector coordination on active defense measures, utilizing existing mechanisms for cooperation such as the industry-led Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs), and the National Cybersecurity and Communications Integration Center (NCCIC) at DHS.**

4. **The National Institute for Standards and Technology (NIST) should develop guidelines, best practices, and core capabilities for private sector activity with respect to assessing the risk of and carrying out active defense measures, with 3-5 different levels of technical maturity linked to certification to carry out certain types of measures, or in the case of third-party vendors, to protect other companies. Such guidelines may be distinct for different industry sectors, and**
this effort at NIST shall be consistent with the work done in 2013-2014 to develop the Cyber-security Framework.

5. Federal agencies that fund cybersecurity-related research and development, including the Departments of Defense, Homeland Security, the Intelligence Community, and the National Science Foundation, should prioritize R&D on the development of new active defense measures (including capabilities that may improve attribution) and assess efficacy of current active defense measures.

6. The Department of State should engage with foreign partners in developing common standards and procedures for active defense measures. This is particularly relevant given the fact that many of the large companies who are affected by cyber threats operate globally, and thus need to protect information on systems in dozens of countries.

7. The Privacy and Civil Liberties Oversight Board (PCLOB) should carry out a review of current and proposed federal government activities related to active defense activities by the private sector, and release a public report on the results of this review.

8. The White House should develop a policy that provides guidance to federal agencies on when and how they should provide support to the private sector with respect to active defense activities, addressing such factors such as the maturity of private sector entities, the nature of the threat actors (if known), and the economic and security-related importance of the infrastructure or information targeted. This latter factor could perhaps be linked to the list of “critical infrastructure at greatest risk” as identified by DHS pursuant to Section 9 of Executive Order 13636. Types of support that are envisioned include information sharing, coordinated planning, intelligence support, and training.

9. The President should issue a directive that codifies the requirements in items 1-6 above and sets clear deadlines for the adoption of them.

Actions for the U.S. Congress

10. Congress should pass legislation to oversee the implementation of the activities in action items 1-7 above, and reinforce the deadlines in statute. Congress should also mandate that the Government Accountability Office review the implementation of this legislation.

11. Congress should reassess language in the CFAA and the Cybersecurity Act of 2015 that constrains private sector activity on active defense, to ensure that low and medium-risk active defense measures are not directly prohibited in statute.

12. Congress should examine whether and how other tools established in law (e.g. indictments, sanctions, trade remedies) can be utilized in support of protecting the private sector against malicious cyber actors. Executive Order 13694 (“Sanctions Related to Significant Malicious Cyber-Enabled Activities”) from 2015 is a good example of this principle in practice, but there are other tools that can be utilized in support of cyber deterrence and active defense.

Actions for the Private Sector

13. Private sector companies should work together and take the lead in developing industry standards and best practices with respect to active defense measures within their sectors and industries. Such efforts should be undertaken on an international basis, involving a broad set of major companies from all regions of the world.

14. Companies should develop policies at the C-Suite level for whether they want to engage in certain types of active defense measures in response to hypothetical future attacks, instead of simply reacting after they have suffered a data breach or other form of cyber attack. Companies should develop an operational template, based upon a thorough risk assessment and analysis of industry standards and best practices, that can be integrated into a broader cyber strategy and incident response protocols. These policies must be incorporated
15. Industry groups should examine best practices for coordination between Internet service providers, web hosting services, and cloud service providers and their clients on active defense, leveraging the fact that these service providers often have contractual, pre-authorized access to their clients’ networks for routine business purposes. Such service providers may be well positioned to carry out active defense measures against cyber threats to their clients.

The report concludes with a call to action on this issue and a brief examination of future trends that may impact the evolution and development of active defense policy and procedures. The report includes several appendices that support the report’s core analysis, including a review of U.S. law, vignettes that provide a global perspective on active defense (in the United Kingdom, France, Estonia and Israel), and a glossary of terms.

TO GENERATE THE FRAMEWORK contained in this report, the Center brought together a diverse group of expert stakeholders, convening a Task Force whose members have backgrounds in the private and public sectors, and are thought leaders in the areas of technology, security, privacy, law, and business. Led by the four Task Force co-chairs, the Active Defense Task Force met on four separate occasions for working sessions. The meetings addressed a range of fundamental themes and challenges, including: the policies and laws governing active defense against cyber threats both inside and outside the United States; existing and emerging technologies for protecting against cyber threats targeting the private sector; and corporate best practices for protecting and defending systems.

Task Force co-chairs and Center staff also consulted widely with stakeholders across the country, including financial sector executives in New York City, senior U.S. government officials in Washington, D.C., and a range of Silicon Valley technologists, through interviews conducted either in person or by telephone. The majority of these interactions and exchanges took place under the Chatham House Rule in order to encourage free and full discussions of the issues under study.

Ultimately, the many findings produced by these expert conversations were distilled and developed into key principles that were debated, refined, and placed in context in this report. While the members of the Task Force found common ground and reached agreement on many aspects of this discussion, they did not reach a consensus opinion on all issues discussed below. The findings and recommendations of this report, as informed by the deliberations of the Task Force, were therefore produced and refined by the co-chairs, and should be interpreted in the context of the additional views of Nuala O’Connor, as expressed in Appendix I of the report.
Participants

Task Force Co-Chairs

Admiral Dennis C. Blair
Former Director of National Intelligence; Chairman and
CEO, Sasakawa Peace Foundation USA

Secretary Michael Chertoff
Former Secretary of Homeland Security; Co-Founder and
Executive Director, the Chertoff Group

Frank J. Cilluffo
Director, Center for Cyber and Homeland Security;
Co-Director of the Project

Nuala O’Connor
President and CEO, Center for Democracy & Technology

Project Staff from the Center for Cyber and Homeland Security

Deputy Director & Co-Director of Project
Christian Beckner

Associate Director & Research Director of Project
Sharon Cardash

Policy Analyst
Taylor P. Brooks

Presidential Administrative Fellow & Project Coordinator
Alec Nadeau

Active Defense Task Force

Stewart Baker
Steptoe & Johnson

David Heyman
Tektonics Global, LLC

Cheri McGuire
Standard Chartered Bank

Christopher Ballister
IBM

Jason Healey
Columbia University, School for
International & Public Affairs

Angela McKay
Microsoft Corporation

Robert Chesney
University of Texas School of Law

General Reynold Hoover
National Guard Bureau

James Mulvenon
Defense Group, Inc.

Robert Corcoran
Zurich Insurance Group

Irving Lachow
Mitre Corporation

Robert Nichols
Covington & Burling, LLP

Rajesh De
Mayer Brown

Peter LaMontagne
Novetta

Michael Papay
Northrop Grumman

Timothy Evans
Johns Hopkins University, Applied
Physics Laboratory

Nathan Lesser
National Institute for Standards
and Technology

Harvey Rishikof
Crowell & Moring

Nathaniel Fick
Endgame

Ariel Levite
Carnegie Endowment for
International Peace

Keenan Skelly
Circadence

Brian Finch
Pillsbury, Winthrop, Shaw, Pittman

Jane Holl Lute
Former Deputy Secretary of
Homeland Security

General Kenneth Todorov
Northrop Grumman

Zachary Goldman
Center on Law & Security, New York
University School of Law

Matthew McCabe
Marsh

Cory Wilson
Law Enforcement Policy Advisor

Geoff Hancock
Advanced Cybersecurity Group

Michael Zweiback
Alston & Bird, LLP
This report—the result of a research initiative featuring the perspectives and expertise of the Center for Cyber and Homeland Security’s Active Defense Task Force, as led by the Task Force co-chairs—presents a practical framework for industry and government action that will enhance the private sector’s ability to defend its most valuable data and assets in the context of modern cybersecurity imperatives.