PROJECT REPORT

INTO THE GRAY ZONE

The Private Sector and Active Defense against Cyber Threats

Center for Cyber
& Homeland Security
THE GEORGE WASHINGTON UNIVERSITY

INTO THE GRAY ZONE

The Private Sector and Active Defense Against Cyber Threats

Project Report
October 2016

Center for Cyber
& Homeland Security
THE GEORGE WASHINGTON UNIVERSITY

Center for Cyber and Homeland Security
2000 Pennsylvania Avenue NW
Washington, DC 20052
www.cchs.gwu.edu

Table of Contents

Foreword and Acknowledgements

PRIVATE SECTOR ENTITIES operate today on the front lines of cyber conflict, targeted by a variety of hostile actors that seek to steal and misappropriate their intellectual property, degrade their infrastructure, and disrupt their business activities. Despite this reality, the options available within the private sector for responding to cyber threats are outdated and constrained. The status quo is reactive in nature and advantages the attacker. The time has come for the private sector, working together with governments, to flip the equation and enhance its ability to counter such cyber threats.

A key element of a cyber strategy for the private sector is **active defense**, a term that captures a spectrum of proactive strategic and technical cybersecurity measures that are the focus of this report. Such measures—if developed and used within a carefully defined legal and policy framework that accounts for technical risks and companies' differing capabilities—provide a powerful tool for addressing cyber threats to the private sector.

There are two major challenges for private sector cybersecurity that active defense capabilities would address. The first is related to the cyber threat. Simply put, threats are expanding in persistence and consequence and we cannot solely rely on defensive measures and "firewall" our way out of this problem.

The second challenge has to do with the mismatch between capabilities and authorities between the public and private sectors. While the U.S. government will always play an important role in cybersecurity, it lacks the resources to fully defend the private sector in the digital realm. But the current legal and policy environment for companies to defend themselves is ambiguous, making it risky for businesses to utilize active defense tools that may be effective in addressing malicious cyber attacks. The United States' efforts to articulate an effective cyber deterrence posture are also constrained by this ambiguity about active defense.

Many American policymakers, recognizing the private sector's significant role in the nation's cybersecurity, have led numerous calls for greater public-private partnerships. However, such initiatives have to date been incomplete, focusing on information sharing, best practices, and post-incident investigation. There is a need for government to partner with the private sector in developing and implementing a framework for active defense. Such a framework would allow forward-leaning and technologically advanced private entities to effectively defend their assets in cyberspace, while at the same time ensuring that such actions are embedded within a policy and legal framework that confirms government oversight, ensures that privacy and civil liberties are not infringed, and mitigates technical risks. America cannot accept the cybersecurity risks of a vulnerable private sector or continue to maintain an inadequate cyber deterrence posture.

It is our hope that the framework offered in this report will help to crystallize thoughts, build consensus, and ultimately, spur requisite action related to private sector active defense by the U.S. government and American business executives. In January 2017, the new President and Administration will undoubtedly face a host of challenges that demand priority attention, and the present subject should rank among them given the powerful interplay between national security and economic security.

This report places the current cyber threat in its larger strategic context and then assesses the role of private sector active defense in addressing such threats. With this in mind, the report proposes a framework that defines the most prevalent active defense measures and places them along a spectrum of relative risk and impact, indicating where close coordination with the government becomes necessary for responsible private action. This framework will help actors in the public and private sectors understand and operationalize active defense against cyber threats and is contextualized through careful analysis of relevant policy, technology, and law. The implications of each measure are especially considered in light of the rights and freedoms of Internet users that such a framework should support to the greatest extent. Next, we specify a series of key recommendations that are segmented by target audience (the executive branch, Congress, and the private sector). Finally, the report concludes with a brief discussion of issues for future consideration, followed by standalone appendices that contain, respectively, a deeper dive into the legal dimension, selected global perspectives on active defense (Estonia, France, Israel, and the United Kingdom), and a glossary of relevant terms. The findings and recommendations of this report were distilled by the co-chairs and project staff and do not necessarily represent the views of each member of the Task Force. Co-chair Nuala O'Connor has submitted additional views (Appendix I).

This initiative was made possible by the generous financial support of The William and Flora Hewlett Foundation and the Smith Richardson Foundation. In addition the George Washington University Center for Cyber and Homeland Security and the Task Force co-chairs are grateful for the time, resources, and insights contributed by the Members of the Active Defense Task Force and many other stakeholders—both organizations and individuals—that participated in the workshops, panel discussions, interviews, research, and drafting that helped to shape the ideas contained in this report. To be clear though, it should be noted that this report does not represent a consensus viewpoint of the participants in the task force process.

While it is not practicable to name each and every instrumental contributor to this endeavor we would be remiss if we did not single out at least a few, while at the same time acknowledging the vital expertise that many provided on a not-for-attribution basis across a range of disciplines including technology, security, privacy, law, and business. The law firm of Covington & Burling, LLP and in particular partner Robert Nichols and his team of associates conducted substantial

legal research for this project on a pro bono basis. Orin Kerr, the Fred C. Stevenson Research Professor at the George Washington University Law School also served as a legal consultant.

The Department of Justice's Computer Crimes and Intellectual Property Section, the United States Secret Service, The Carnegie Endowment for International Peace, Endgame, Johns Hopkins University Applied Physics Laboratory, Microsoft, Mitre, and Novetta provided tailored briefings to the full Task Force. The Johns Hopkins University Applied Physics Laboratory and the William and Flora Hewlett Foundation lent meeting space to the Task Force for two of the four working sessions. Building on the deliberations of the Task Force, this report was primarily drafted by the staff of the Center for Cyber and Homeland Security, including Christian Beckner, Taylor P. Brooks, Sharon Cardash, and Alec Nadeau; Joseph R. Clark and Rhea Siers contributed critical insights. Throughout the life of this project, Alec also worked tirelessly to coordinate the Task Force's activities and provide logistical support.

The issues discussed in this paper are complex, and attempt to address and balance the views and interests of a diverse group of stakeholders from the U.S. government, various elements of the private sector (notably the tech sector and the financial sector), academia, privacy and civil liberties organizations, and international governments. While we have not proposed a path that reconciles all of the conflicting interests from these different stakeholders, we believe that our proposals can bring them closer together, aligning interests and moving toward productive solutions to common challenges. Our aim was to help chart a constructive course forward through this complicated terrain, and in this, we hope we have succeeded.

Washington, D.C. - October 2016

Task Force Co-Chairs:

Admiral Dennis C. Blair
The Honorable Michael Chertoff
Frank J. Cilluffo
Nuala O'Connor

Participants

Task Force Co-Chairs

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

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

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

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

Christopher Ballister
IBM

Robert Chesney
University of Texas School of Law

Thomas Corcoran
Zurich Insurance Group

Rajesh De
Mayer Brown

Timothy Evans
Johns Hopkins University, Applied Physics Laboratory

Nathaniel Fick
Endgame

Brian Finch
Pillsbury, Winthrop, Shaw, Pittman

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

Geoff Hancock
Advanced Cybersecurity Group

David Heyman
Tektonics Global, LLC

Jason Healey
Columbia University, School for International & Public Affairs

General Reynold Hoover
National Guard Bureau

Irving Lachow
Mitre Corporation

Peter LaMontagne
Novetta

Nathan Lesser
National Institute for Standards and Technology

Ariel Levite
Carnegie Endowment for International Peace

Jane Holl Lute
Former Deputy Secretary of Homeland Security

Matthew McCabe
Marsh

Cheri McGuire
Standard Chartered Bank

Angela McKay
Microsoft Corporation

James Mulvenon
Defense Group, Inc.

Robert Nichols
Covington & Burling, LLP

Michael Papay
Northrop Grumman

Harvey Rishikof
Crowell & Moring

Keenan Skelly
Circadence

General Kenneth Todorov
Northrop Grumman

Cory Wilson
Law Enforcement Policy Advisor

Michael Zweiback
Alston & Bird, LLP

Executive Summary

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 Cybersecurity 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.[128] 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 within the companies' broader commitment to and investment in their own traditional cyber defense programs.

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.

1 Background on the Cyber Threat, Responses to the Threat, and Active Defense

IN THE PAST SEVERAL YEARS, top national security leaders and executives in the private sector have argued that cybersecurity vulnerabilities are a major threat to their organizations' missions and to U.S. national security.[1] Indeed cybersecurity is increasingly listed as a top concern for CEOs and other corporate executives.[2] Media outlets are flooded with reports of massive breaches at consumer-facing companies, advanced cyber espionage, and cyber attacks on critical infrastructure.[3] Gone are the days in which the average individual thought about cybersecurity only when his or her credit card was compromised. Instead, a February 2016 Gallup poll found that 73% of Americans considered cyberterrorism to be a critical threat to the United States.[4] *These developments are in part the result of the difficulties in deterring malicious cyber activities, something the United States and many other nations have struggled to do.*[5]

Recently, observers have noted a significant escalation in the frequency and efficacy of strategic malicious cyber activity. In the private sector, targets have ranged from Sony Pictures to Yahoo, to political organizations. With recent breaches at the Internal Revenue Service, the Office of Personnel Management, and various state agencies, it is clear that government organizations at all levels are also targets of cyber threat actors.[6] The sheer number of successful malicious cyber actions that defenders have faced up to this point has increased the level of frustration many have with traditional cybersecurity measures and has raised the question of what entities can do to adequately defend their interests in cyberspace. As companies collectively lose billions of dollars to intellectual property theft, lose the right to control the use of their most personal information, and generally lose their sense of trust and security online, the feeling that current cyber defenses have failed them is inescapable. In order to preserve public trust in the Internet and its underlying utility, 21st century cybersecurity practices must evolve alongside threats to national security, economic vitality, privacy, and human rights. This report will demonstrate how new cybersecurity practices and strategies can enhance cyber defense in the private sector.

America is at an inflection point in cyberspace. U.S. government agencies and private sector companies have developed and benefited from some of the most advanced capabilities in cyberspace. But these same entities are vulnerable to disruptive cyber incidents, and are under constant threat from a variety of actors. One key element of a broad effort to address this challenge is more clearly defining the private sector's role in cybersecurity, not only with respect to information sharing and defensive activities, but more broadly with respect to "active defense," a set of operational, technical, policy, and legal measures that are the subject of this report.

What is the Cyber Threat?

Before turning to a more detailed discussion of active defense later in this paper, we first need to consider and assess the types of cyber threats that are targeting the private sector.

America's most sophisticated cyber adversaries are the nation-states of Russia, China, Iran, and North Korea.[7] In some instances, these states may use their own military and intelligence services to conduct cyber exploitation, but increasingly states are acting through proxies to whom they may provide funding or other tacit support.[8] Foreign states and their proxies are joined by a variety of other cyber threat actors including criminal enterprises, hacktivists, and terrorists that are engaged in malicious cyber activities against U.S. entities.[9]

Those who use cyber means to exploit or attack computer systems in America and other countries act out of a variety of political, ideological, and geostrategic motivations. Malicious actors may seek power, prestige, money, or some combination of the three.[10] Nation-states may hope to gather intelligence on their adversaries or damage a rival's critical infrastructure in times of conflict. Criminals tend to be active wherever they can make a profit and where the costs of doing business are low. Terrorist organizations have used the Internet to recruit and radicalize, but undoubtedly aspire to more destructive cyber-enabled attacks.[11] Hacktivists often use cyber capabilities to pursue a political end.[12] Across all cyber threat actor types and motivations, malicious cyber activity is increasing in scale and sophistication, often enabled by advanced and shared capabilities. Regardless of their specific capabilities and motivations, cyber threats undermine the trust and stability of the Internet, corrupting its inherent value.

Cyber Threats to National Security, Economic Security, and Privacy

The effects of cyber threats are not, however, limited to an abstract assault on the Internet as a concept. The cyber threat landscape tends to jeopardize a number of American interests, including national security, economic vitality, human rights, and privacy.[13] National security concerns were raised in 2013 when Iranian hackers gained access to the servers that controlled a dam in Rye, New York.[14] Activities like these are a form of intelligence preparation of the battlefield, tailored to the cyber domain, and could presage attempts to target and disrupt even more significant critical infrastructure in the United States. The disruptive effects of the malicious cyber activities on Ukraine's electricity grid in 2015 highlight precisely why such attacks must be taken extremely seriously.[15]

Beyond the threat to U.S. national security posed by malicious cyber attacks and espionage is the constant threat against the U.S. private sector. The security of the American economy is of fundamental importance not only to the United States, but to the entire world. Yet cyber espionage, theft, and sabotage against the private sector are rampant. Former NSA Director Gen. Keith Alexander described the cyber theft of American industrial information and intellectual property as the "greatest transfer of wealth in history."[16] In recent years, the cost to the U.S. economy from malicious cyber activities has increased.

The cyber threat landscape tends to jeopardize a number of American interests, including national security, economic vitality, human rights, and privacy.

Malicious cyber actors have particularly targeted certain industries, such as the financial sector. In 2012, a disruptive series of Distributed Denial of Service (DDoS) attacks targeted 26 major U.S. banks over a period of four months, causing significant financial losses. In August 2016, Roman Seleznev of Russia was

convicted for cyber-criminal activities that caused over $169 million in losses to 3,700 financial institutions.[17] The recent fraudulent manipulations of the SWIFT interbank messaging system led to millions of dollars in losses and fears that the entire global banking system could be at risk of manipulation.[18]

Malicious cyber actors are frequently targeting valuable intellectual property (IP), the protection of which is necessary to a well-functioning market economy. In 2013, the IP Commission Report found that 20% of American jobs were in IP-intensive industries and that the negative effects of IP theft in one sector can have secondary effects throughout other sectors, threatening U.S. economic security.[19] This highlights a larger concern that although industrial sectors may have differing cybersecurity capacities, a major vulnerability in one sector could have serious impacts across the board.[20]

The cyber-related economic threat poses a significant strategic threat to American security. Recent estimates put the cost of cyber attacks against private business to be between 0.64% and 0.9% of the United States' gross domestic product.[21] If those estimates are accurate, cyber-attacks did between $120 and $167 billion dollars of damage to the U.S. economy in 2015. Given the ongoing rapid growth in cyber attacks, this trend is likely to continue, if left unchecked.[22]

Numerous cyber exploitations represent an assault on the individual right to privacy. Recent incursions into the private networks of Target, Sony Pictures, Yahoo, and the Democratic National Committee represent a few of the many particularly threatening cyber operations from a privacy perspective.[23] In these hacks, malicious cyber actors exploited and released sensitive consumer information, private communications, and intellectual property. In order to preserve public trust in the Internet, 21st century cybersecurity practices must evolve alongside threats to national security, economic vitality, privacy, and human rights.

What is Being Done to Safeguard Against Cyber Threats?

One key aspect that differentiates cybersecurity threats from other security threats is the extent to which the government appears unable to adequately protect the private sector. It is not that the government is uninterested in cybersecurity threats to the private sector, or that it lacks the ability to contribute in some degree to cyber defense and incident response. However, cyber threats are much more common, persistent, and diverse than traditional security threats, and in many cases, are far less costly to execute. Facing a scarcity of resources, government agencies must carefully prioritize their initiatives and responses. Furthermore, security researchers generally agree that the advantage in cyber conflict lies with the attacker, making it an even more resource-intensive task to defend crucial assets and raise costs on otherwise unpenalized malicious actors in cyberspace.[24] While the government has worked with industry to develop cybersecurity guidelines and will often assist with the investigation of major breaches, it cannot assume primary responsibility for defending the private sector, as it does in the face of most other threats.

The private sector is therefore on the front lines of cyber competition and conflict today. Businesses never anticipated the scale to which they would be responsible for defending their interests against the military and intelligence services of foreign countries. Yet in many instances, that is exactly what certain industries and companies are facing. Private entities are generally no match for the resources and expertise of a foreign state; this is particularly true with respect to cybersecurity, where firewalls and security patches are often

not enough to keep out hackers, and the inherent advantage rests with the attacker. A sophisticated adversary can easily disrupt a service, steal assets, or even destroy data held on private servers. Even non-state malicious actors have increased their sophistication in recent years, at times nearing a level of sophistication previously thought only achievable by the most capable of state actors.

Despite the limitations of defensive measures, it is important to note that private sector companies that implement basic practices of cyber hygiene can prevent the vast majority of malicious cyber activity. Companies are increasingly adopting security controls that will allow them and government partners to focus more resources on countering advanced threats—ones where active defense capabilities come into consideration.

The Anatomy of Exploitation and Attack

Although security policy experts have put much thought into how to preserve and protect U.S. national security, economic security, human rights, and privacy from cyber threats, the nature of evolving technologies make this an ongoing and challenging task. In order to understand why malicious actors have such an advantage in cyberspace, and why defending against them remains so problematic for both the government and the private sector, it is helpful to have a basic understanding of how computer network exploitations and computer network attacks occur.

The Cyber Kill Chain, originally developed by the Department of Defense, can serve as a strong starting point for this type of analysis.[25] The model divides the life cycle of a hack into three major steps: preparation, intrusion, and active breach; and was developed as a guide for gathering intelligence on cyber attacks that would help defenders secure their systems throughout the life-cycle of a hack. This report's "anatomy of exploitation and attack" outlined in Figure 1, is a slightly modified model that incorporates details included in other analyses of hacker behavior, such as the InfoSec Institute's Cyber Exploitation Cycle.[26] Critics of the cyber kill chain argue that it relies too heavily on perimeter-based defense techniques and is therefore less helpful when it comes to describing socially engineered attacks, the insider threat, and other modern methods of cyber exploitation.[27] While it was never intended to be operationalized against all types of cyber exploitation, the true weakness in applying the kill chain to cybersecurity is not that the model overemphasizes intrusions at the perimeter, but rather that those who use the model limit themselves to cybersecurity tools that are almost exclusively geared towards perimeter security. This report will frame the anatomy of exploitation and attack in such a way that is directly relevant to the private sector and can begin to guide cybersecurity practitioners away from limiting notions of network defense.

A modified version of the kill chain concept is a useful tool to analyze the stages of a cyber threat at which certain defensive tactics become relevant. Thus, the anatomy of exploitation and attack will serve as a reference point, as this report continues, to demonstrate where emerging cybersecurity practices can disrupt and defeat cyber threat actors. Furthermore, it will help to visually demonstrate how new cybersecurity practices can fill the gaps that intrusion-based cyber defenses currently leave exposed.

Key U.S. Interests In Cyberspace

Although the number and sophistication of cyber threats continues to grow, the United States has thus far escaped a significant cyber attack that has seriously damaged its critical infrastructure or way of life. How long this relative sense of security can last is unclear. Over the past decade, the arsenal of offensive cyber measures has grown unbounded; botnets, DDoS attacks, ransomware, remote access tools, encryption-based exploitation tools, social engineering, and zero-day exploits are the standards of the day.[28] It will only be a matter of time before an adversary successfully capitalizes on these advantages and carries out an attack that damages and disrupts critical infrastructure. This type of asymmetric threat environment requires a carefully calibrated strategic response and calls for a broader cyber deterrence strategy. Not all threats are deterred in the same manner, however,

so the U.S. must develop and implement a clearly articulated strategy tailored to the unique threat against the private sector.

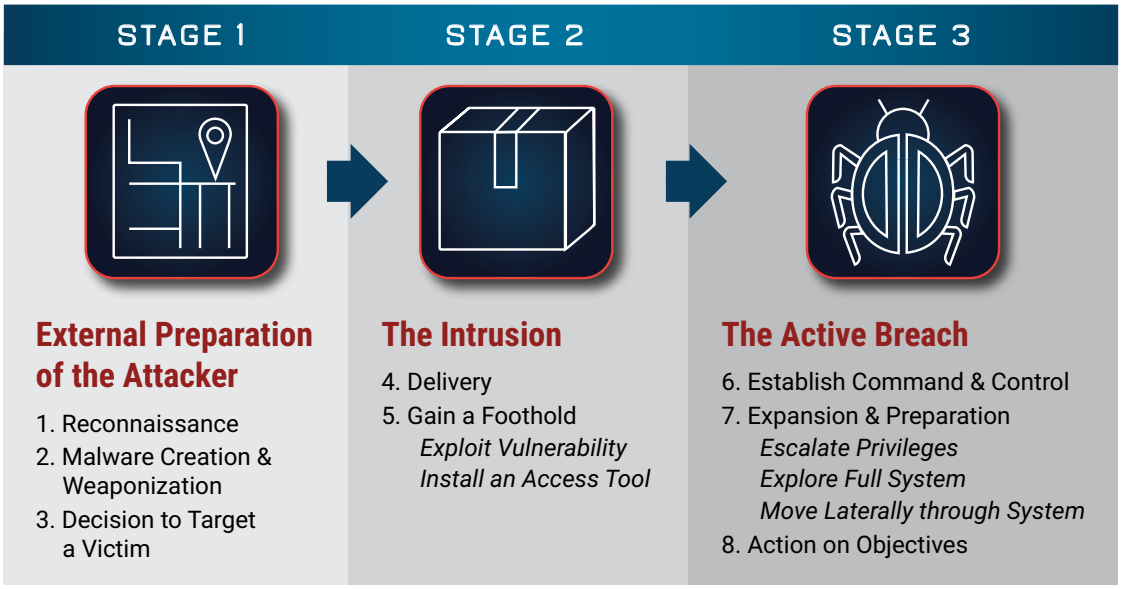
At present, it is unlikely that any state or non-state actor possesses the combination of capabilities and interests necessary to threaten American sovereignty and freedom of action in or through cyberspace. While the recent Russian hacks on U.S. political entities and related information operations have caused a stir this election cycle, the complexities and redundancies of the U.S. electoral system make it relatively resilient to systemic cyber manipulation. While there is some threat that even the doubt created by information warfare campaigns can impact American sovereignty, thought leaders and government officials have so far been able to dispel any type of widespread distrust in America's electoral system.[29]

Though the fundamental sovereignty of the United States is not at issue, other key strategic interests, such as U.S. economic security, may be more susceptible to cyber threats. Private sector enterprise, including technological advancement, protects national economic security by fueling economic development, nurturing the growth of military capabilities, and fostering geopolitical influence.[30] Over time, unchecked cyber-enabled theft of private sector data and assets could pose a strategic risk and threat to a nation's economic security. The cyber-enabled misappropriation of private sector assets may occur directly as a result of the immediate transfer of actual wealth from victim to attacker. Alternatively, such misappropriation could be of an indirect nature, from the manipulation of sensitive information that damages a company's relationships, value, or reputation. The effect of either type of attack would be to give competitors a competitive advantage. Depending on the nature of such an attack and its target, its effects could devastate individual firms, damage whole sectors, or weaken entire economies.

Effective Deterrence and Active Defense

Since U.S. economic security has a unique susceptibility to malicious cyber activities, the U.S. should craft a cyber deterrence policy that is more focused on protecting the private sector. Effective cyber deterrence will require that government and private sector actors have a robust and diverse array of options, including a more permissive policy on the private use of

FIGURE 1. ANATOMY OF EXPLOITATION AND ATTACK



active defense measures. The question of objective is straightforward. The U.S. must cut the drain on the economy and private sector caused by malicious cyber activities. Developing a near-term strategic response within such a context requires prioritizing the most pressing threats facing the private sector.

The long-term strategic response must include a cyber deterrence strategy that actually denies benefits and imposes costs. While actors in the public and private sectors currently attempt to deny benefits to attackers using passive and perimeter-centric defense measures, these defenses alone are outmatched by today's offensive capabilities. Furthermore, while the government has attempted to contribute to such a deterrence posture by imposing costs on malicious actors, this strategy is complicated by the difficulties associated with attribution, the limited resources and tools available to governments seeking to punish international actors, and other geopolitical factors.[31]

Historical patterns and modern technology have created a strategic imperative: American policymakers must develop a framework to defend against the misappropriation of wealth from the private sector. The duality of a global economy in which economic partners may simultaneously be geopolitical adversaries makes articulating an effective cyber deterrence posture complex and unique. Flexibility, innovation, and careful cooperation will be key.

Many senior national security officials have argued that if America is to deter aggression in cyberspace, it needs to pursue a whole-of-government approach to cybersecurity that closely involves the private sector.[32] Together, the public and private sectors will need to implement more reliable tools for cyber defense and attribution. This will require increased information sharing to support awareness, cooperation to coordinate responses, and the constant cultivation of private-public partnerships to support decision-making. Cooperation, however, is not the solution in and of itself. In order to ensure that adversaries cannot effectively threaten the strategic interests of the United States in cyberspace, America must move beyond cybersecurity models that focus on outdated passive defense measures.

In order for what is truly a whole-of-nation cybersecurity strategy to succeed, the private sector must be allowed and encouraged to build upon its innovative capabilities and advanced resources to pursue a strategy of active cyber defense.

Active Defense: How the Term has Developed and How it Should be Used Going Forward

Active Defense is a term that has been in use within the national security and defense communities for a number of decades. Since its origins in the Department of Defense and its later application to the cyber domain, it has taken on a whole host of meanings. Today, the legacy of its various and evolving interpretations obscures the utility of a term in a sea of conflicting definitions. A brief history of the evolution of the term is helpful to provide some context before this report proposes a recommended definition for consistent future use in the cyber context.

The distinction between active and passive defense was first discussed many decades ago in the context of the military's traditional physical land, sea, and air defenses.[33] Passive defenses were understood to be those that provided a limited amount of defense against an adversary without requiring military engagement.[34] A traditional passive defense measure might be a hardened bunker or other add-on security measure that depleted an adversary's resources by requiring extra effort on the part of the adversary to achieve its goal.[35]

In the 1970s, the term active defense began to emerge in U.S. Army lexicon during discussions of land warfare tactics. While analyzing the 1973 Arab-Israeli War, U.S. Army General William E. DePuy, Commander of the Army Training and Doctrine Command, used the term to describe a defensive technique based on mobility.[36] The defender would wear down the attacker by "confronting him successively and continuously with strong combined arms teams and task forces fighting from mutually supported battle positions in depth throughout the battle area."[37]

In order to achieve mobility, the defender needed to

leverage "military intelligence, and indicators to identify an attack, respond to the attack or against the capability within the defensive zone or contested area."[38] Even at the time, the term was controversial and hotly debated. The use of counterattacks by the defender was restricted to only the "contested area" against the threat itself. Active defense was directed "against the capability, not the adversary."[39] In its original sense, active defense techniques gave the defender the ability to quickly adapt to the environment in real-time to address attacks in a proactive way. Over time, the definition used by the military was formalized in the Department of Defense *Dictionary of Military and Associated Terms* as "the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy."[40]

Active and passive defense definitions were developed separately, and before the term "cyber" was ever incorporated into military doctrine.[41] Experts have struggled to translate the traditional definitions of active and passive defense into perfect analogues in the cyber context. The SANS Institute has crafted a definition based upon the protective nature of passive defenses: "systems added to the architecture to provide consistent protection against or insight into threats without constant human interaction."[42] A collection of cooperative automated systems such as firewalls, antivirus or anti-malware systems, intrusion detection and prevention systems, and others fall into this category.[43]

It is similarly challenging to translate physical conceptions of active defense into the cyber domain. SANS has defined cyber active defense as "the process of analysts monitoring for, responding to, learning from, and applying their knowledge to threats internal to the network."[44] The scope of this definition is limited and therefore this report will introduce, in the following section, a robust definition of active defense with clear examples. The SANS definition precludes hacking back and other activities that occur outside the network, focusing instead on dynamic adaptability as a tool to react quickly to threats overcoming passive defenses.[45] Like the traditional definition in land warfare, the activity is confined to the "contested area" of the defender's internal network.

For the private sector, discussion of the term active defense has been regularly linked with discussions of the Computer Fraud and Abuse Act (CFAA). In 1989, five years after the CFAA became law, Robert Morris Jr., an MIT graduate student, became the first private citizen prosecuted for releasing what was arguably the first major computer virus distributed through the Internet, the Morris Worm.[46]

Since that time, there have been many CFAA prosecutions aimed at those who have gained unauthorized access to computer systems, raising concerns in the private sector over the extent to which private firms may defend themselves using techniques that may involve information or computer systems external to one's network without express government authorization.

The private sector, faced with escalating losses from malicious cyber threats, has been discussing the idea of active defense for years. Perhaps the first widely known instance of a private use of active defense measures occurred in 1999 when Conxion, Inc., a web service company that hosted the World Trade Organization's servers, took action against a denial of service (DoS) attack targeting its servers. Tracing the source of the malicious traffic, Conxion reflected the incoming traffic back at the source, flooding the server with its own outgoing traffic; effectively imposing a "reverse" DoS attack on the attacker.[47]

In 2004, the company Symbiot, Inc. released the first commercially available security platform that could "execute appropriate countermeasures" against a cyber threat. By offering graduated response levels, the system offered a range of options for the user that exceeded the "passive" defenses of other security products. Symbiot's press release called their new tool, the "Intelligent Security Infrastructure Management System" (iSIMS) the "equivalent of an active missile defense system" that would allow the user to fight "fire with fire."[48] In keeping with their military analogy, the company also issued a paper on the Rules of Engagement that discussed the application of the military principles of necessity, proportionality, and countermeasures, linking the practice of active defense measures with the military's historic understanding of the term.[49] Importantly, the Symbiot product offered a series of graduated responses, not just a "hack back" solution. iSIMS could implement, among other techniques, challenging procedures, honeypots, quarantines, reflection, and blacklisting upstream providers in an escalating series of options.[50]

Despite this broad array of options, during the time since the release of iSIMS product, there have been many debates over the issue within the private sector, academia, and government. Today, when active defense is discussed, too often the discussion shifts to "hacking back"—offensive cyber measures that are beyond the scope of what we define as permissible activity in this report.[51] This report seeks to more clearly articulate the terminology and public dialogue around the topic.

Defining Active Defense for 21st Century Cybersecurity

Given its diverse usage over a number of decades, when security experts, policymakers, and academics use the term active defense in a cybersecurity context, they tend to have in mind a wide variety of definitions. This lack of a common definition complicates discussion surrounding active defense and precludes meaningful progress on developing a commonly understood framework for its implementation. This is especially counterproductive when it comes to developing policy related to cyber active defense in the private sector.

It is similarly challenging to translate physical conceptions of active defense into the cyber domain.

Sound practice related to private sector active defense is also obstructed by businesses' increasingly common use of third party services to host sensitive data and information outside of their own infrastructure. This development undermines network defense strategies

that are based on clearly defined network perimeters and areas of direct ownership. Thus, any relevant definition of active defense will need to consider the gray areas in which businesses may be forced to defend their data on a third party's infrastructure. With this in mind, the report proposes the following characterization of 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 Upper and Lower Bounds: Passive Defense and Offensive Cyber

In order to fully contextualize this definition of active defense, it is necessary to define its upper and lower bounds. Cyber activities can produce effects that manifest within the actor's own network, outside the actor's own network, or both. The Center's definition of active defense includes activities that fall across that range, including some activities that manifest effects, whether logical or physical, outside of a particular actor's own network or systems.

Activities that produce effects solely within an actor's own networks are often referred to as passive defenses. They primarily involve the use of perimeter-focused tools like firewalls, patch management procedures, and antivirus software. These can be installed and left to function independently. Passive defenses can also include procedures like white or blacklisting and limiting administrative authorities. While passive defenses are necessary for a sound cybersecurity regimen, they are insufficient by themselves to defend against the most advanced cyber-aggressors.

On the other extreme are those activities occurring outside the actor's network, and that are aimed at coercing action, imposing costs, degrading capabilities, or accessing protected information without authorization; these could be characterized as offensive.[52] "Hacking back" to retrieve or delete stolen data or to gain information about an attacker's tools, techniques, procedures, and intents fits into this category, as would a retaliatory DDoS attack, the exploitation of a system to extract intellectual property, or the use of malware to damage a system, such as in the case of Stuxnet.[53] [54] As in other domains of conflict, private sector actors should not be authorized to use these types of tools, except in limited circumstances in cooperation with or under the delegated authority of a national government.

The Spectrum of Active Defense: A Continuum of Activities

Active defense measures include those which typically fall between these upper and lower definitional boundaries. Such activities may cross the threshold of the actor's own network borders, and produce effects on the network of another. These activities, taken in pursuit of a variety of objectives that may be either offensive or defensive, affect the confidentiality, integrity, or accessibility of another party's data. They are no longer passive in nature, and their characterization depends upon the intent or objective of the actor implementing them. Activities aimed at securing one's own systems, or preserving operational freedom could be characterized as defensive in nature.[55] Disrupting a malicious botnet, sinkholing traffic from a malicious IP address, and other activities that are taken in direct response to an ongoing threat would fall within this category.[56]

Examples of active defense measures can be found in Figure 2, and are ranked according to their relative impact and risk from left to right.[57] (Definitions for each of these active defense measures can be found in Figure 3). The activities towards the far left of Figure 2 are relatively common and low-risk active defense options such as information sharing and the use of honeypots or tarpits. A computer security expert who uses a honeypot on his or her network can, assuming that the decoy fools the attacker, observe attack techniques and use these observations to inform defenses on the defender's actual network.

While less common, cyber denial and deception is another low-risk defensive technique that can be used to observe attacker behavior, tailor other active defense techniques, and improve incident response capabilities. It can involve concealing and making apparent both real and false information to skew an aggressor's understanding of the information contained on a computer system, vulnerabilities in that system, and defenses deployed on a network.[58] The process of hunting for and removing threat actors who have already breached fortified perimeter defenses is surprisingly uncommon, yet a relatively impactful cybersecurity measure for its low level of risk. Hunting is as much about having actionable procedures and responses in place for eliminating threats as it is about exposing them, whether they be active or dormant in a network.

Towards the middle of the active defense spectrum are activities that carry more risk, in that they generally involve operations outside of one's network, and have the potential to lead to minor collateral damage or privacy concerns if used without the requisite level of precision. These activities include beaconing, the use of dye packs,[59] and intelligence collection in the deep web and dark net. Beacons are pieces of code that are embedded into files that contain sensitive information. They can be operationalized in two main ways. First, less impactful beacons will simply alert the owner of a file if an unauthorized entity attempts to remove that file from its home network, acting as a built-in burglar alarm. Second, more aggressive beacons are designed to return to the victim information about the internet addresses and network configurations of the computer systems that a stolen document is channeled through, ideally assisting with attribution and forensic evaluation of remote devices.

Increasingly, network defenders are realizing that the information that travels through the dark net can be helpful to inform defensive strategies and alert information security officials of a breach. This realm of the Internet—in which websites are dissociated from traceable servers, user anonymity is common, and information travels between trusted networks of peer groups—is popular for criminal trade in stolen information and malware services, and thus offers a promising trove of human intelligence possibilities for network defenders. For example, a bank's security team can search through illicit marketplaces and compare the personal or financial information on sale with the information the bank keeps on its custom-

FIGURE 2. ACTIVE DEFENSE: THE GRAY ZONE

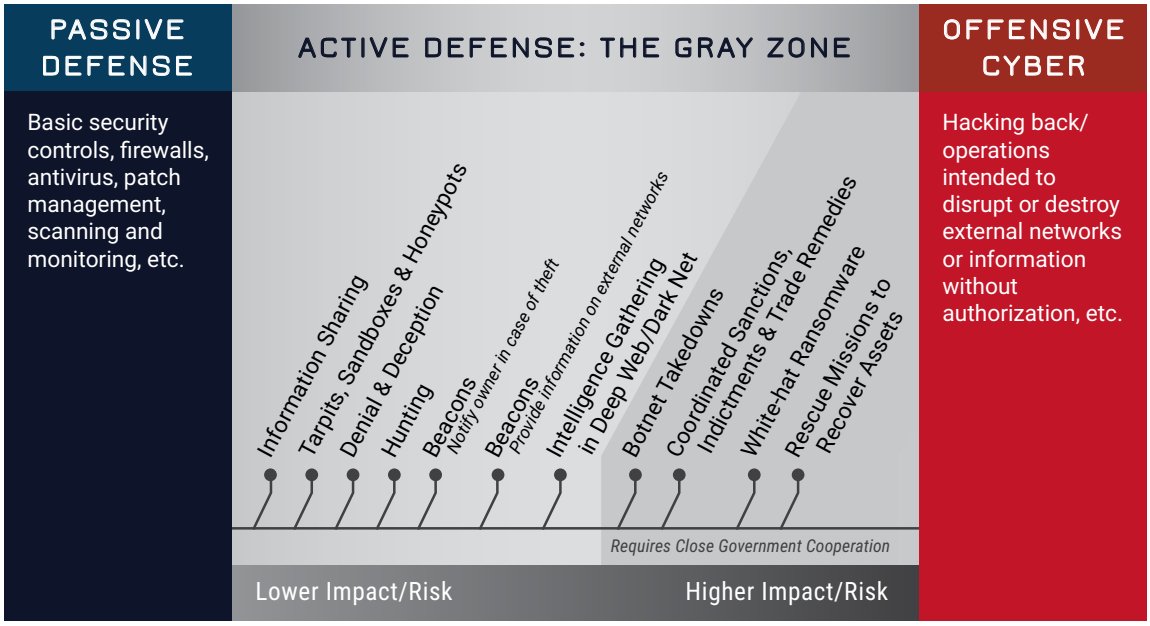


FIGURE 3. ACTIVE DEFENSE TECHNIQUES DEFINED

Lower Impact/Risk

Information Sharing
The sharing of actionable cyber threat indicators, mitigation tools, and resilience strategies between defenders to improve widespread situational awareness and defensive capabilities.

Tarpits, Sandboxes & Honeypots
Technical tools that respectively slow hackers to a halt at a network's perimeter, test the legitimacy of untrusted code in isolated operating systems, and attract hackers to decoy, segmented servers where they can be monitored to gather intelligence on hacker behavior.

Denial & Deception
Preventing adversaries from being able to reliably access legitimate information by mixing it with false information to sow doubt and create confusion among malicious actors.

Hunting
Rapidly enacted procedures and technical measures that detect and surgically evict adversaries that are present in a defender's network after having already evaded passive defenses.

Beacons (Notification)
Pieces of software or links that have been hidden in files and send an alert to defenders if an unauthorized user attempts to remove the file from its home network.

Beacons (Information)
Pieces of software or links that have been hidden in files and, when removed from a system without authorization, can establish a connection with and send information to a defender with details on the the structure and location of the foreign computer systems it traverses.

Intelligence Gathering in the Deep Web/Dark Net
The use of human intelligence techniques such as covert observation, impersonation, and misrepresentation of assets in areas of the Internet that typically attract malicious cyber actors in order to gain intelligence on hacker motives, activities, and capabilities.

Botnet Takedowns
Technical actions that identify and disconnect a significant number of malware-infected computers from the command and control infrastructure of a network of compromised computers.

Coordinated Sanctions, Indictments & Trade Remedies
Coordinated action between the private sector and the government to impose costs on known malicious cyber actors by freezing their assets, bringing legal charges against them, and enforcing punitive trade policies that target actors or their state sponsors.

White-hat Ransomware
The legally authorized use of malware to encrypt files on a third party's computer system that contains stolen information in transit to a malicious actor's system. Public-private partners then inform affected third parties that they have been compromised and are in possession of stolen property, which they must return in order to regain access to their files.

Rescue Missions to Recover Assets
The use of hacking tools to infiltrate the computer networks of an adversary who has stolen information in an attempt to isolate the degree to which that information is compromised and ultimately recover it. Rarely successful.

Higher Impact/Risk

ers and their accounts. If the security team discovers a significant match, then it is likely that a hacker breached their network and successfully stole sensitive data without raising the alarm. Defenders, now alerted to the presence of a network vulnerability, can seek to shore up cracks in their security architecture and boot intruders off their system before any more information is compromised.

Those active defense activities that approach the rightmost extreme of the spectrum in Figure 2 are the most aggressive. Private entities should only utilize such measures, as the figure suggests, when working in close cooperation with the government. These activities include sinkholing botnet traffic and taking down the infrastructure of botnets or criminal forums. Botnet takedowns have, up to this point, proven to be some of the most effective partnerships between government and private actors seeking to cooperate on more forward-leaning categories of active defense. The numerous instances of cross-sector and inter-jurisdictional partnerships that have operated under legal authorities to successfully sinkhole botnets provide hope that public-private coordination is possible in cyberspace.[60]

The group of non-technical actions that appear in Figure 2, coordinated indictments, sanctions, and trade remedies, are not active defense measures in the purest sense, but require mention in this conversation due to the technological underpinnings that facilitate requisite attribution. The investigative tools that are required to confidently attribute malicious cyber activity to an entity can be invasive and thus require close cooperation with the government. The legal and trade implications that follow from such activities would not be possible in many cases without private sector contributions and can contribute significantly to a cyber deterrence posture.

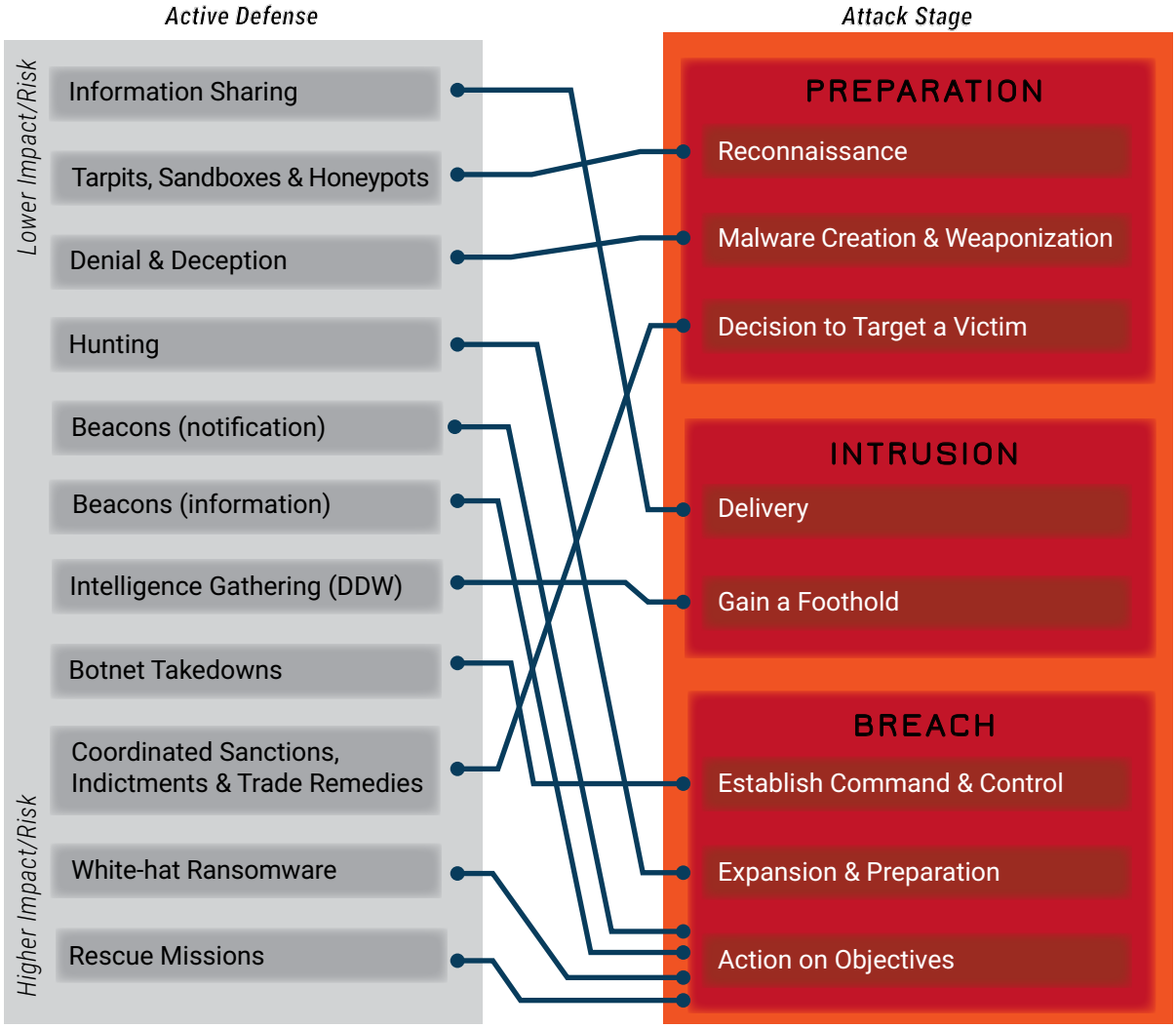
Other active defense measures that are more aggressive and risky include white hat applications of ransomware, and the often discussed and widely inadvisable "rescue mission" for information that has already been stolen from one's network. While the malicious use of ransomware has become one of the most worrisome trends in cybersecurity over the past year, security experts have considered the possibility of using similar tools to encrypt stolen data that is in transit on a third party's network. In such a manner, they could inform a third party that hackers had compromised their network and were using it to transmit stolen data. Instead of the warning screen that usually tells victims to pay a ransom in bitcoin, white hat ransomware would inform network administrators that they should contact law enforcement, which can retrieve the stolen information and then remove the ransomware from the third party's computers. There are legal risks, however, with this approach, as well as a new security risk that such warning notices could be spoofed for phishing attacks that lead to further compromises.

While technically feasible, operations in which defenders attempt to retrieve stolen information from adversary networks, even when the intent is not to alter or destroy any of that adversary's other legitimate data, are not likely to succeed and are inadvisable. The difference between such "rescue missions" and the much maligned "hack back" is in the intent of the defender: whether he or she is looking to retrieve what was stolen or to inflict damage. Both are high risk and often ill-fated from the start. The moment an advanced adversary captures stolen information, they are likely to protect it by replicating and hiding it within their network or backing it up offline. Due to the low likelihood of achieving a beneficial outcome, even if government partners were to be involved, such operations are again, inadvisable.

Active Defense as it Intervenes in the Anatomy of Exploitation and Attack

Together, these activities make up the current spectrum of private sector active defense measures. Figure 4 demonstrates how active cyber defense strategies can fortify the efforts of security experts to disrupt attacks at various stages within the anatomy of exploitation and attack. The lines in Figure 4 show where certain active defense measures have significant capacity to interdict cyber exploitations and attacks. Many of these measures impact adversary behavior at multiple stages, but for clarity's sake, Figure 4 explicitly shows only those connections with the highest impact. Passive defense strategies alone usu-

FIGURE 4. WHERE ACTIVE DEFENSE INTERDICTS A CYBER ATTACK



ally focused on preventing and detecting intrusions. Alternatively, active defense techniques allow organizations to potentially interrupt attackers in all three stages of a hack. When defenders fail to implement active defenses, cybersecurity cannot reach its full potential to deny benefits to attackers throughout the entire duration of the hack.

While discussion surrounding specific security technologies or techniques is necessary to illustrate different aspects of active defense, it is important to note that such technologies are likely to have relatively short shelf lives. The key takeaway from this discussion is therefore not the specifics of how a honeypot works or how to sinkhole a botnet. Instead, the goal is to show how such tools and techniques exemplify the concept of a range of active defense activities that can be helpful in addressing current cyber vulnerabilities. Broadly speaking, active defense measures can help to directly inform threat assessments and cybersecurity priorities, protect a business' "crown jewels" within a network, assist in reliable attribution, recover stolen information, and neutralize threats.

Active Defense Case Studies

Before turning to a broader policy discussion of the private sector and active defense against cyber threats, it is

useful to examine two instances where private entities have used active defense measures (as we have defined them) to mitigate or disrupt cyber threats. Both of these brief vignettes are drawn from open source information, and provide useful insights into the kinds of threat scenarios that necessitate active defense and the ways in which private actors have legally and effectively implemented active defense strategies. With the conclusion of each case study, this report discusses broad takeaways that relate each case to the calculations that today's executives must make when shaping their approaches to cybersecurity and cyber incident response.

Google's Response to Operation Aurora

The response of Google to the Chinese-linked hacking campaign that security researchers at McAfee dubbed, "Operation Aurora," provides a detailed case study of how a particularly skilled private sector actor has used active cyber defense measures to protect its security interests. After Google became aware of a "highly sophisticated and targeted attack" on its networks and corporate infrastructure in late 2009, it decided that a timely response to the breach was necessary. Therefore, internal security teams began a campaign to assess the scope of the breach and investigate the attackers themselves. They found that these attackers had targeted user accounts, many of which were associated with individuals the Chinese government considered to be political dissidents; and Google's source code, a critical corporate asset and significant piece of intellectual property.[61] If the hackers had been able to alter the source code while remaining undetected, they could have built vulnerabilities directly into Google's product plans.

As a large technology firm, Google's leadership decided it had the resources to support a mission to operate outside of its network to track down the attackers. Its search led to a command and control server in Taiwan. Google found that the attacks were likely being controlled from China and that Google was among a group of at least 30 other targeted companies.[62] With this information in hand, Google took the unprecedented step of sharing its findings with law enforcement, the intelligence community, the companies involved, and even the public.[63]

Google's decision to carry out this type of response and subsequently make it public carried with it legal and reputational risks. Although the details of the Aurora hack on Google are well documented, it remains unclear how exactly Google traced and entered the Taiwanese server. If, as has been reported, it entered the foreign computer without authorization, Google's actions could be interpreted as a violation of the Computer Fraud and Abuse Act (CFAA), potentially subjecting it to civil or criminal liability. However, U.S. government agencies chose not to take action against Google, and instead admonished China while praising the value of Google's investigative efforts.[64] To date, the government has not prosecuted a single company for engaging in active defense measures similar to Google's, although it does warn others of its authority to do so.[65]

Google's response to Operation Aurora demonstrates that the private sector can be a useful partner to the government in this endeavor.

The impacts of Google's response to Operation Aurora on the conversation surrounding active defense are manifold. First, Google's apparent use of a beaconing technology and its network investigation techniques demonstrate that attribution is not impossible and that the private sector can be a useful partner to the government in this endeavor. Second, this example must be considered in the context of Google's size, influence, and technical sophistication. Not just any private business could have supported this type of response and not all businesses should consider engaging in such a response.

Third, the lack of an identifiable victim of Google's countermeasures, whether the intended targets of such

action or innocent third parties, likely contributed to the fact that the Department of Justice never brought suit against Google. Had a private company's actions caused damage on the network of a readily identifiable victim with commercial interests in America or Asia, they would have likely led to prosecution, regulatory action, or civil action under the CFAA or foreign legal authorities. In such a counterfactual, Google's actions and the legal fallout could have considerably tarnished the company's reputation and bottom line. All executives engaging in active defense must consider these potential consequences in conjunction with the risk of taking no action at all. After all, failure to act entirely could result in even more significant consequences to a business' reputation and bottom line. C-suite executives should take each of these considerations into their risk analysis when developing a cyber strategy.

The Dridex Botnet Takedown

The takedown of the Dridex/Bugat botnet is another helpful case study of how defenders have successfully implemented active defense strategies. The partnership between international law enforcement agencies and private sector actors to dismantle the command and control (C&C) infrastructure of Dridex illustrates how multilateral partnerships that draw on diverse partners with a range of authorities and expertise can disrupt cybercrime and penalize criminals.[66] Dridex was a banking Trojan that was spread through spam emails. It would steal online banking credentials that criminals would use to fraudulently transfer money into accounts they controlled. This botnet disproportionately affected small- and medium-sized businesses in the U.S. and Europe.[67]

The Dridex botnet, which security researchers first discovered and significantly analyzed in November of 2014, breached thousands of organizations across 27 countries and led to losses in the UK of about $30.5 million and $10 million in the U.S.[68] Cyber criminals used this malware to fill the void left by the similarly purposed Gameover Zeus botnet and designed it so that it could avoid common antivirus software.[69] These designs, coupled with its use of a resilient peer-to-peer C&C structure, made it a challenging botnet to combat. However, by October of 2015, U.S. and U.K. government officials announced that the botnet had largely been dismantled through close cooperation between multiple private sector entities and other government agencies.[70] Together they had redirected the malicious commands of the C&C servers to a sinkhole that the Shadowserver Foundation administered.[71] The Dridex takedown operation did not remove malware from infected machines, leaving bots vulnerable to re-infection and future manipulation.[72] As in similar botnet takedowns, individual users and their security vendors were responsible for cleaning up their own computer systems. Coordinating remediation efforts continues to be a major burden to implementing botnet takedowns.[73]

Significantly, American law enforcement obtained a court order before taking action against the botnet's C&C servers. Coinciding with the takedown announcement, the US Justice Department indicted a Moldovan national, Andrey Ghinkul, on a number of counts related to operating Dridex, which included "criminal conspiracy, unauthorized computer access with intent to defraud, damaging a computer, wire fraud, and bank fraud."[74] In February of 2016, the U.S. successfully extradited Ghinkul from Cyprus.[75]

There are three major points to take from this case that are broadly applicable to discussions surrounding cyber threats to the private sector and active defense. First, the fact that Dridex led to significant financial losses, disproportionately affecting small- and medium-sized businesses, demonstrates the severity and ubiquitous nature of the cyber threat to all actors in an economy. Big banks and giant retailers are not the only victims in the current threat landscape. Second, the Dridex takedown exemplifies how public and private entities pool resources in order to tackle a common threat. Because sinkholing botnet traffic can be aggressive in the context of computer trespass norms, law enforcement and the private sector sought legal approval before taking action. Finally, this case shows that attribution in cyberspace can be successful and can lead to significant legal costs for cyber criminals. Imposing real costs on these criminals is crucial to removing critical talent from cybercrime circles and to deterring individuals from engaging in such crime.

2 The Current Policy, Legal and Technology Context

THE PRIVATE SECTOR TODAY is situated on the equivalent of the front lines of battle: sophisticated and determined actors ("advanced persistent threats") pose serious threats to U.S. companies.[76] Foreign nation-state security and intelligence forces and their proxies, either actively sponsored or passively sanctioned, increasingly target U.S. businesses for a range of reasons and purposes including computer network exploitation (CNE) and computer network attack (CNA). These actors seek, among other things, to disrupt normal operations, to steal intellectual property, and to map networks that support critical U.S. infrastructure and services such as the electric grid.[77]

Yet the extent to which the private sector can act to thwart these and other cyber threats is limited by policy and law. The current legal framework in the U.S. maintains certain domains of action in this regard as the exclusive preserve of government, which in turn gives rise to interdependencies between the targeted entity and federal authorities. Robust and adaptive partnerships between the public and private sectors are therefore required to meet ongoing evolving and future cyber challenges.

Appendix II to this report identifies and analyzes the legal instruments and common law principles that are most relevant to this study. It includes two U.S. statutes, the CFAA and the *Electronic Communications Privacy Act* (ECPA), as well as an overview of the common law theories of trespass, self-defense, and necessity.[78] Collectively, these instruments and principles provide a useful starting point for analyzing the legality of accessing a computer that you (the hacker or his target) do not own or have authority to operate. Pursuant to statute, whether (or not) access is "authorized" is pivotal, and is factually determined on a case-by-case basis. The body of law on this issue is ambiguous however, and parties to litigation have invoked (with varying degrees of success) supplemental legal principles and doctrines—such as necessity, defense of property, and implied consent—to make their case before the courts.[79] *What is clear is that under U.S. law, there is no explicit right to self-defense ("self-help") by private companies against cyber threat actors.*

Since "authorization" is the key requirement for any actor to access any computer network or system, a victim who wishes to implement offensive measures against an attacker must be authorized to intrude upon or act within the attacker's network. Since this is unlikely to ever be the case unless previously authorized by contract, U.S. law is commonly understood to prohibit active defense measures that occur outside the victim's own network. This means that a business cannot legally retrieve its own data from the computer of the thief who took it, at least not without court-ordered authorization. Moreover, measures that originate in your own network—but whose effects may be felt outside your perimeter—may also fall afoul of the law. While the exercise of prosecutorial discretion by the Department of Justice may temper formal legal bounds, it should also be understood that U.S. attorneys will not prioritize the

prosecution of attackers over defenders, meaning that anyone who oversteps places themselves in potential legal jeopardy.[80]

Multiple considerations are said to underlie the restrictive nature of the U.S. regime. The law seeks to protect third parties that could suffer significant incidental damage and prevent escalation of the conflict, with possible concomitant effects on U.S. foreign relations. Without concerted de-confliction efforts undertaken in advance, ongoing U.S. law enforcement investigations could be hindered, or security research could be affected. And, to the degree that the activity pursued by the targeted private party reaches into foreign jurisdictions, those (non-U.S.) laws may also be offended raising concerns over the possibility of foreign penalties and extradition requests. The difficulty of attack attribution in the cyber context presents a further risk, giving rise to the possibility of harm to third parties, resulting from mistaken belief in their guilt.

Juxtaposed against this legal framework is an ecosystem of rapidly evolving technology. Advances in machine learning and machine-speed communications have served to propel automated processes for detecting cyber threats, sharing threat-related information, and responding swiftly. These technologies are being used increasingly in both the public and private sectors, and across them.[81] Internet-based cloud technologies, too, will continue to open up options for businesses whose size and accompanying resource level might otherwise constrain their capacity to defend themselves against cyber threats. Cloud computing is a boon to small and medium-sized businesses as it allows them to scale up or down, and pay accordingly, based on their prevailing need for specific services.[82] The point is not academic as threat actors have targeted companies of all sizes.[83]

Some companies have pursued measures outside the United States in order to secure their assets from cyber threats in a manner that U.S. law would not countenance.

It is also reasonable to expect that, over time, R&D will generate ever-new technologies that can enhance the private sector's ability to meet and defeat cyber threats. On the other hand, threat actors will also find ways to exploit new technologies to their advantage, such as the Internet of Things, which dramatically expands the potential surface of attack.[84]

While technology is a double-edged sword that can serve both to protect and harm, the bounds of the prevailing legal framework can be—and have been—pushed by those with an appetite for risk, fueled by the desire to practice self-help. Companies with substantial resources, for instance, have pursued measures outside the United States in order to secure their assets from cyber threats in a manner that U.S. law would not countenance.[85] The circumstance arises in part because companies are unwilling to passively place their fate in the hands of the U.S. government. This lack of confidence is premised on multiple concerns, including serious doubt that governments possess either sufficient skill or the sustained determination and resources required to pursue perpetrators effectively, and provide adequate remediation—which is essential to deterrence and prevention, moving forward.

These points are well taken in that government cannot be expected to successfully deter cyber attackers targeting U.S. public and private sector interests everywhere, all the time. The challenge is compounded, ironically, by the private sector's ability to outbid the government for highly skilled cyber experts. A sense of mission is powerful, but the appeal to public service in the national interest (along with other factors that animate individuals to join the civil service) have yet to result in filling the many critical cybersecurity positions and functions in government that remain open.[86] In the longer term, this situation could be redressed by growing the pool of qualified candidates, by deepening and expanding U.S. efforts to encourage our young people to undertake and continue studies in science,

technology, engineering, and mathematics (STEM). But companies need a fix for today, because the existing framework which structures the relationship between the public and private sectors is not sufficiently responsive to the needs of business, given the current cyber threat climate and tempo.

Yet, private sector actors are less engaged than they could be, despite being a potential source of the very resources and expertise that the government lacks. By and large, companies are not pursuing—either independently or in partnership—the actions that are needed to create a strong deterrence posture benefiting from active defense. This disengagement is due to many things: legal ambiguity, risk aversion, limited resources, lack of coordinated leadership, and lack of awareness of active defense.

Legal ambiguity exists at the international level as well, where the framework applicable to the cyber domain remains nascent. The Council of Europe Convention on Cybercrime (the Budapest Convention) includes a definition of "Illegal Access" that may help to define the boundaries of permissible active defense measures.[87] Several countries are developing their own approaches to the question of active defense (see Appendix III). Global norms, though emergent, are at present not sufficiently developed so as to be determinative, which compounds companies' quandaries.[88]

Those who take bold (and arguably incautious) steps to protect stolen assets will, even if initially successful in practice, achieve but a Pyrrhic victory if a company's hard-earned goodwill is dissipated by ensuing litigation. Moreover, taking independent action or joining forces with others to frustrate and deter cyber threat actors presumes that businesses have the wherewithal (technical and otherwise) to do so; but this is not a given for many in a tough economy in which many and varied company goals and objectives compete with one another, and there are only so many hands on deck to achieve them. At the senior executive level, furthermore, cyber knowledge and the drive to prioritize measures (*e.g.,* prevention and mitigation) in this domain are uneven. Within and across industry sectors there is significant variation in levels of awareness about active defense, as well as in the level of resources (amount and quality) that are available.[89]

There are a number of current initiatives that illustrate how the private sector can play a lead role in thwarting cyber threat actors. Examples include the Cyber Threat Alliance (CTA), which strives to share "actionable threat intelligence" among its members.[90] Notably, the CTA has acted jointly to expose and counter ransomware attacks that caused damage worldwide, valued at more than $300 million.[91] Without sustained and coordinated leadership though, laudable efforts such as this will re-

main limited in their effects and result only in hit and miss rates of success.

The upshot is that private entities, which did not get into business to defend their information and infrastructures against sophisticated cyber actors, are forced to do just that. This is an unsustainable position.

In the remainder of this report, we put forward a new framework that attempts to addresses the challenges outlined here—most fundamentally, that the status quo leaves America vulnerable to significant cyber threats. With the private sector often looking to be more aggressive, but hamstrung by the potential for serious risks and unintended consequences, U.S. companies need clarity on what they can and cannot do. These parameters should be defined in advance, as the product of a careful deliberative process—rather than in the heat of the moment, when a mindset to avenge may exist, or a cycle of regression may take hold due to a hack that has unintended consequences.

3 Genesis of the Framework

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 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.

4 A Framework for Active Defense Against Cyber Threats

AFTER THIS EXTENSIVE PROCESS of consultation and review, the report offers a risk-based framework for private sector active defense that strikes a balance between the risk of inaction in the face of escalating cyber intrusions, versus the risk of overly aggressive responses that could escalate, backfire, or harm innocent third parties.

The core of this framework is the spectrum of active defense measures defined in Figures 2 and 4 of this report. These measures are 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. This framework can guide and influence both short-run decision-making (*i.e.* how to respond now to an attack), as well as longer-term investment and capacity-building.

The framework seeks to maximize the effectiveness of the private sector's ability to defend its most valuable data and assets. We propose to expand the private sector's latitude for action, so that companies may take limited yet appropriate actions to protect themselves against various types of cyber threats, including the theft and exfiltration of data. But we also propose to embed these authorities to act within a policy and legal framework that is risk-driven and accounts for companies' relative capabilities to engage in such actions. We propose that such private sector actions should be considered within a broader framework of public-private cooperation on cyber threats, so that government legal authorities and investigative capabilities can be used in concert with private sector action, and to ensure de-confliction of efforts. The implementation of such a framework will raise costs for and reduce benefits to attackers, dissuading and deterring threats over time.[92] It will also ensure that measures are proportional to the threat and will restrain harmful or unlawful actions. For those actors already engaged in active defense measures, it will provide guidance to ensure their measures fall within the bounds of the law.

This framework recognizes that a broad suite of technical and non-technical tools is applicable to the countering of cyber threats to the private sector. In addition to purely technical active defense measures, this includes such activities as information sharing, and intelligence collection, as well as broader policy tools such as sanctions, naming and shaming through technical attribution, indictments, and trade remedies. These non-technical activities and tools are informed by technical approaches to cybersecurity and cannot be excluded from conversations on active defense and cyber deterrence. While such actions are typically the purview of government actors, the resources of the private sector are valuable when implementing such policies in cyberspace due to the Internet's dispersed and bottom-up design. Closer cooperation between domestic, private actors and government agencies that implement such policies is thus desirable. In fact, coordination between government and business

is required in most realms of active defense. A strong framework will help to alleviate the advantage that malicious actors gain from current ambiguity in terms of who takes the lead in defending businesses in cyberspace. The framework would also provide for greater transparency and accountability in private sector active defense.

The framework also balances 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. While a strong framework for responsible active defense will bolster the tools that the private sector can employ to safeguard the privacy of their customers' sensitive personal information, the importance of guaranteeing the responsible use of active defense measures cannot be overstated. Activities that extend beyond the networks that a company is authorized to access raise legitimate privacy concerns (among other issues) for innocent third parties, so the framework must ensure that any measures taken by the private sector are proportional to the threat and limited in scale, scope, duration, and effect. By providing a clear framework for these activities, practices that exceed or circumvent the framework's carefully crafted best practices may be curtailed before undue infringement on the privacy rights of innocent parties can occur. There are a variety of oversight mechanisms and legal reporting requirements that could be utilized to ensure that such considerations are integrated into the framework.

A 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 actions is warranted. As discussed later in the paper, government should work with the private sector to establish such a risk-driven methodology, developing it through an open, consultative process.

Key Actors in the Active Defense Framework

Before looking at how this framework can be used, we need first to understand the capabilities and interests of the key actors within it. The framework's first relevant set of actors includes the various businesses that make up the U.S. private sector. The Task Force quickly recognized that due to the enormous diversity of private entities operating in the United States, not all sectors operate at the same level of sophistication. Referring only to the capacity of the "private sector" as a whole is an overgeneralization. Indeed, there is no "single" private sector. While many "mom-and-pop" shops operate with only the most basic firewalls installed on their computers, others, like the defense, technology, finance, and energy sectors, have developed and actually employed comparatively advanced cyber defense capabilities to protect their networks.

Some cyber capabilities cross into a "gray area" of activities that fall below the level of hacking back but still push the limits of current U.S. law.

Many large companies utilize advanced cyber capabilities that cross into a "gray area" of activities that fall below the level of hacking back but still push the limits of current U.S. law. In 2013, the FBI investigated whether a number of U.S. banks had used active defense techniques to disable servers in Iran that were conducting malicious attacks against their networks.[93] No charges were brought, but major banks reportedly advocated strongly for such activities.[94] The next year, an industry coalition including Microsoft, Symantec, and Cisco dismantled a sophisticated, allegedly Chinese-backed APT known as Axiom,[95] removing the group's malware from 43,000 computers around the world. Today, companies in the United States and Israel are selling increasingly advanced cybersecurity solutions to top financial and defense firms that push the limits of measures that can be fairly called "passive defenses."[96]

Many private sector actors are increasingly implementing their own progressively aggressive defensive

measures because they believe the government has failed to offer adequate protection.[97] Advanced actors within the private sector often believe their own abilities to react quickly to defend their networks make them more effective defenders of their data than law enforcement or other government entities. For private entities operating in a market where safeguarding customer privacy is a top concern and reaction times are often measured in nanoseconds, waiting for the government to come to the rescue is not enough.[98] If a proper balance is struck that allows the private sector to react to threats to its networks without overly burdensome laws and policies, the private sector can be a vital player in ensuring the nation's economic security.

The other key actors incorporated into the active defense framework are the various executive branch agencies (including law enforcement and regulatory agencies) that have cybersecurity responsibilities and Congress. Although the state has historically been responsible for protecting its citizens and private sector from external threats, due to limited resources and available personnel, it is unlikely the government will ever be able to fully respond to cyber threats that do not directly and substantially threaten the national interest.[99] Protection of public networks alone already consumes much of the government's cybersecurity bandwidth. At the current rate, the government is failing to address the most common and widespread threats to the private sector: those that can overcome firewalls and other passive security measures, but fail by themselves to rise to the level of national security threats.[100] Unfortunately, while such malicious activities do not garner the full attention of the government, the sum of their impacts can grow to such a degree that they do collectively pose a major threat to economic and national security. This dangerous reality will only intensify in coming years. As the rapid development of the "Internet of Things" suggests, the private sector faces a growing attack surface and an increasing array of vulnerabilities inherent in their products, services, and operating procedures.[101]

Despite the growing security gap, the government is the sole actor with the prerogative to engage in techniques like "hacking back" that involve accessing a system outside a defender's networks with the intent to disrupt or destroy parts of a computer system. Though the CFAA prohibits "unauthorized access" to a computer, Congress specifically excluded from coverage "lawfully authorized investigative, protective, or intelligence activity" of law enforcement and intelligence agencies.[102] The Department of Justice is clear

that without law enforcement authorization and outside of direct cooperation, hacking back is a violation of the CFAA, subject to civil and criminal penalties.[103] Conspicuously absent from the legality discussion by DOJ officials are those active defense activities that fall below the level of hacking back, such as intelligence gathering, beaconing, and sinkholes.[104]

Operationalizing the Active Defense Framework

The first step necessary in creating an effective environment for the use of active defense techniques by the private sector is for the government to eliminate the legal "gray areas" by more clearly and explicitly defining which types of techniques fall within the bounds of the law. This can be accomplished by assigning a legal or other categorical status to certain characteristics of an active defense technique. There are a number of relevant characteristics that could be considered in such an analysis, including temporal, functional, effects-based, and location-based factors.

The first step is for the government to eliminate the legal "gray areas" by more clearly and explicitly defining which types of techniques fall within the bounds of the law.

A first consideration is the point during the attack at which the defender utilizes the active defense measure. Is the technique used preemptively, during, or after an attack?[105] Stopping an ongoing attack is likely to be considered more legitimate than a retaliatory or otherwise post hoc attempt to recover or deny the attacker the benefits of their attack. A second useful consideration is the technique's intended function. Is the purpose to collect intelligence on a threat, to prevent an attack from ever occurring, to end a network attack, to mitigate damage, retrieve stolen assets, or impose costs on the attacker?[106] A corollary consideration is how the technique affects the confidentiality, integrity, or accessibility of data. Society may find some effects, such as "observation" or "access" more acceptable than the "disruption" or "destruction" of data.[107]

A cyber activity may also be categorized based on its effects and location.[108] Is the effect felt purely within the defender's network, or on outside networks such as on the attacker's or that of some third party? Though such activities are at times desirable, such as the automatic removal of malware or patching of a vulnerability, any damage to the data or networks of an innocent third party would need to be remedied. Cloud computing and the distributed architecture of the Internet itself make identifying specific individuals difficult, particularly if malicious actors are using proxies to carry out their activities.

Next, is the active defense measure authorized, whether by an oversight body, law enforcement, or the owner of the affected network? As discussed before, botnet takedowns have become a common mechanism for the government and private sector to cooperatively address cyber threats. These operations have primarily been conducted in a partnership with law enforcement, bolstered by the authority of a court order. Law enforcement and other public sector entities are likely to view a defender's defensive measures in a more favorable light if they are given a cooperative role or otherwise have some oversight authority.

Finally, is the entity that is carrying out the measure capable of doing so in a way that maximizes its efficacy and minimizes the risk of negative consequences, such as collateral damage to other systems or networks or potential escalation?

Both the government and the private sector can benefit from careful consideration of these factors. The government should institute a strong declaratory policy detailing the characteristics of active defense techniques it believes fall within the bounds of the

law. The existence of such a declaratory policy would encourage the private sector to carefully consider these factors whenever engaging in active defense measures.[109] With a clear characteristics-based legal framework, it would be possible for a private actor to assess the legality of a particular activity or technique on a case-by-case basis.

The characteristics-based analysis would not be complete without a strong risk assessment process that weighs the risks of using a particular active defense technique against the risk of failing to do so. Such an analysis must be broad and consider not just primary consequences to the information systems involved, but also second and third order consequences such as the privacy rights of those potentially affected. Any newly developed techniques must undergo careful consideration before being implemented to ensure they fall within the bounds of the law and sound policy.

This type of analysis will be useful in expanding the range of options open to the private sector when faced with attacks against their most valuable assets and data. Although flexibility and adaptability in the face of technological change are hallmarks of this type of characteristics-based analysis, there are certain principles that should serve as bright lines for the extreme ends of the spectrum of acceptable cyber defensive measures.

First, "hacking back" by the private sector to intentionally cause substantial harm and destroy other parties' data is clearly unauthorized and rightly prohibited. These types of activities clearly fall within the type of behavior prohibited by the CFAA and other relevant U.S. laws like the Cybersecurity Act of 2015 and the Federal Wiretap Act. From a policy standpoint, these techniques are likely to escalate incidents because they are likely to be disproportionate, difficult to adequately contain, often retributive, and imprecise. Activities such as hacking back to retrieve stolen data or infecting the attacker's own systems with malware are likely to be ineffective. Stolen data likely exists in a multitude of locations both inside and outside of the attacker's networks. It is unlikely that an attempt to retrieve stolen data would remove it from every location where it is stored; the risk of escalation in exchange for uncertain gains is simply too high. These types of cyber defense activities should continue to be prohibited.

On the other side of the spectrum are activities such as firewalls, internal traffic monitoring, intrusion detection, hunting, and information sharing systems that identify and target threat signatures and indicators of compromise. These activities primarily involve analysis of the defender's own logs and traffic data to search for malware or other irregularities. Automation of these processes along with vigilant adherence to other cyber hygiene best practices will continue to provide a minimal layer of defensive protection against an onslaught of malicious threats. These activities occur primarily within the defender's own network, and do not intrude on the data or networks of any other party. They are both legal and fundamental to a strong cybersecurity regimen.

Other activities, such as the use of beacons, honeypots or tarpits, remote intelligence gathering, and denial by deception, which may have traditionally fallen within the legal "gray areas," should be analyzed using the proposed characteristic-based approach recommended by the Task Force. As new technologies and defensive techniques emerge, they too should be analyzed on a case-by-case basis in order to ensure they are compatible with the principles outlined above. Any activity must be necessary, proportional, and capable of being minimized to contain potential unanticipated consequences. Before any defensive mea-

sure is implemented, a defender should be required to assert a positive identification of the hostile actor with near certainty, relying on multiple credible attribution methods. These types of considerations, if undertaken by C-suite executives, attorneys, CISOs, and IT professionals allow for the use of a rapid and flexible roadmap for approving defensive measures.

Even without a change in the laws, the Department of Justice and other law enforcement agencies should exercise greater discretion in choosing when to enforce the CFAA and other relevant laws, and should provide clarity about how it intends to exercise such discretion. Companies engaging in activities that may push the limits of the law, but are intended to defend corporate data or end a malicious attack against a private server should not be prioritized for investigation or prosecution. Instead, only the most serious threats deserve prioritized attention. The government has a real role to play when it comes to private sector cybersecurity, but it should use its limited resources to first address corporate espionage, organized crime, and malicious activities sponsored by foreign governments.

To date, the government has refrained from prosecuting any of the firms that have engaged in active defense, even those that purportedly did so without authorization from law enforcement.[110] However, those pioneering the use of active defense techniques have primarily been well-known titans of their industries, such as Google and Facebook, with myriad connections to U.S. government sources. As the number of firms using active defense techniques increases, without significant legal and policy changes and increased clarity and transparency of prosecutorial discretion, the government will likely feel pressured to prosecute defending firms more often.

This pressure can be resisted. In the past, federal agencies have offered guidance on interpreting federal statutes that could impose liability on individuals and companies engaging in cybersecurity efforts. In 2014, the Department of Justice and Federal Trade Commission issued a policy statement declaring that reasonable information sharing for cybersecurity purposes would not be considered a violation of antitrust law.[111] This assurance was codified by the Cybersecurity Act of 2015. Just as prosecutors avoid stifling legitimate cybersecurity research and refrain from overly aggressive enforcement of antitrust law, the government should avoid blocking private defensive measures through an overzealous use of the CFAA's criminal provisions.

The framework also recommends strengthening existing public-private partnerships and creating new processes to facilitate private sector entities' ability to respond to threats to their networks. As discussed above, in recent years, companies have been working hand-in-hand with law enforcement entities to dismantle giant networks of remotely controlled computers used for malicious attacks, called botnets. Botnet takedowns have largely been conducted by major private sector actors working jointly with law enforcement to employ advanced active defense measures against the botnet's command and control servers.[112] In 2013, Microsoft, in cooperation with international law enforcement partners and facilitated by the FBI, successfully dismantled 1,000 networks used by the Citadel Botnet to target a number of major financial institutions.[113] Since 2013, law enforcement and engaged members of the private sector have worked in cooperation based upon the Citadel model of public-private cooperation.

Although botnets will continue to be a problem, these takedowns illustrate just how effective private sector actors can be in defending their own networks from malicious activities while operating within the bounds of the law. Without the fear of legal consequences, security experts were able to implement robust measures to shut down the botnets and remove harmful malware from computers and networks worldwide. This report recommends streamlining this type of process to make the legal procedures necessary to obtain authorization to engage in active defense techniques easier, speedier, and more transparent. Every process should be tailored as narrowly as possible, and draw from lessons learned from previous cooperative efforts.[114]

One tactic to implement this framework may be to grant licenses to certain cybersecurity companies that would allow them to engage in limited active defense techniques.[115] A federally licensed cybersecurity

firm could gather intelligence about a threat at the request of a private company, and either turn it over to law enforcement, "name and shame" the perpetrators publicly, or share the intelligence privately with other relevant parties. Doing so could address certain domestic statutory issues, since these firms might be considered "lawfully authorized" to operate, in compliance with the law enforcement and intelligence exceptions to the CFAA.[116] Analogous to private detectives, security firms, or specialized police[117] used by the private sector and even the U.S. government today, firms like Crowdstrike, Mandiant, and FireEye have already proven to be adept at this type of information gathering.[118] As Jeremy and Ariel Rabkin note, the United States routinely relies on reporting conducted by private firms that may be unlawful in the country where it is conducted.[119] The firms would be liable for any mistakes in attribution causing damage to third parties, incentivizing prudence and caution.[120] Relying upon private actors to act in an authorized manner on behalf of law enforcement or other elements of government, however, could well raise issues under the state action doctrine and Fourth Amendment jurisprudence that would need to be addressed.

Another necessary aspect of an operational active defense framework is a consultative group or process that can facilitate decision-making between the federal government and the private sector. This could either be a formally established federal advisory committee (similar to the Critical Infrastructure Partnership Advisory Council or the National Security Telecommunications Advisory Committee) or a more ad hoc set of processes for public-private consultation on active defense, consistent with the Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government (established pursuant to the Cybersecurity Act of 2015), the National Cyber Incident Response Plan and other operational plans and procedures.

It is also vital to continue to strengthen the existing diplomatic processes of building global norms of responsible state behavior in cyberspace. During the past few years the international diplomatic community has made a number of significant advances in building consensus on what laws, rules, and norms should govern in cyberspace.[121] In 2013 a group of experts representing fifteen countries at the United Nations (UN), including countries like the U.S., China, and Russia, agreed in a consensus report (the GGE 2013) that international law and the UN Charter apply in cyberspace. A follow-on report from an expanded group of UN experts in 2015 (GGE 2015) outlined specific norms, confidence-building measures, and procedures for international cooperation and capacity building.[122] In 2013, another group of experts released the *Tallinn Manual*, the most detailed study of the applicability of international law to cyberspace, with particular attention to the jus ad bellum (right to war) and law of armed conflict.[123]

The framework recommends strengthening existing public-private partnerships and creating new processes to facilitate private sector entities' ability to respond to threats to their networks.

These are welcomed developments in the international discussion and consideration of active defense, but fall short of answering the ultimate question of which active defense techniques are acceptable and which become prohibited without express authorization. There is scarce international law on the matter. The Council of Europe Convention on Cybercrime (the Budapest Convention) criminalizes computer crimes similarly to the CFAA, but has not been ratified by a few of the most advanced cyber powers, including Russia and China.[124] Generally, international law ap-

plies primarily to states, and therefore has little effect on private sector actors engaging in active defense.[125] Absent an international treaty to clarify the matter, and without a harmonized understanding of which active defense techniques are considered acceptable, those who do engage in active defense may be subject to violations of the law of the country hosting the target servers.

Therefore, it is important for such norms of responsible state behavior to develop in cyberspace. A growing consensus on the responsibility of states to stop malicious cyber activities originating from within their territory has been promoted broadly through acceptance of the GGE 2015. An agreement to prohibit cyber-enabled theft of intellectual property was undertaken by China, the U.S., Russia, and the other members of the G20.[126] These agreements strengthen the case for providing private actors with the leeway to defend themselves when governments fail to meet their commitments.[127]

Diplomats, industry leaders, and other experts should capitalize on this progress to build a global set of norms regulating the use of active defense techniques. These norms will be required to complement existing domestic and international legal regimes that exist to regulate consumer privacy, such as regulations promulgated by the U.S. Federal Trade Commission, and major international data privacy agreements such as the E.U.-U.S. data Privacy Shield agreement.

Beyond the development of international norms, governments must continue to play an active role in protecting domestic entities from cyber threats. While this report primarily focuses on the part that a more proactive private sector can play in denying benefits to malicious actors and bolstering America's cyber deterrence posture, imposing costs on aggressors in cyberspace tends to require state involvement. Furthermore, even companies with massive cybersecurity budgets, such as large financial institutions, do not have the capacity or interest to square off against a state-sponsored adversary in a way that encourages escalation or sustained cyber conflict. Therefore, the government must begin issuing consistent and clear statements detailing which malicious cyber activities will warrant American responses, and how such responses will progress in severity. Demonstrating the capacity and willingness to act in accordance with such statements are also crucial to cyber deterrence. Such progress would help to address some of the more significant threats in cyberspace, allowing private sector efforts, including the responsible use of active defense, to focus on more manageable threats.

5 Implementing the Framework: Key Near-Term Policy Recommendations

THE ESTABLISHMENT of such a framework for active defense against cyber threats is unlikely to emerge quickly or efficiently; it is unlikely in the near-term that there will be a single event that will realign private and public sector incentives and catalyze the development of such a framework. However, there are a number of specific actions that can be undertaken by government agencies and by key private sector companies to shift the policy and legal context for active defense. This section recommends a set of actions which taken together, will shift the policy environment more closely toward one that integrates active defense measures as useful, risk-based tools to counter cyber threats.

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 Cybersecurity 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.[128] 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 within the companies' broader commitment to and investment in their own traditional cyber defense programs.

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.

Collectively, these fifteen recommendations will move the U.S. government and key private sector stakeholders closer to the adoption of the active defense framework envisioned in the last section.

6 A Call To Action

THE TIME FOR ACTION on the issue of active defense is long overdue, and the private sector will continue to be exposed to theft, exfiltration of data, and other attacks in the absence of a robust deterrent. When private sector companies have a capability to engage in active defense measures, they are building such a deterrent, which will reduce risks to these companies, protect the privacy and integrity of their data, and decrease the risks of economic and societal harm from large-scale cyber attacks. We cannot afford to wait any longer on these issues; instead, public and private sector actors need to work together to clarify the gray zone between doing nothing and hacking back, and then utilize available tools effectively and responsibly. Such efforts will shift risk back to our cyber adversaries, and ultimately serve as a deterrent to further action and the basis for multilateral coordination between and among the public and private sectors, leading to enhanced cooperation and mutual protection against cyber threats.

7 Active Defense Considerations for the Future

THIS REPORT IS A SNAPSHOT of active defense and its broader implications as they exist today. However, it is important to recognize that this field will be constantly evolving—including from the standpoint of technology and law. With respect to technology, key questions for the future include: how active defense will be impacted by the Internet of Things (IOT), cloud computing, increasingly distributed enterprises, and the changing capabilities and intentions of threat actors? Certainly the IOT will expand exponentially the opportunities for adversaries to attack. At the same time, from the defender's perspective, the task of identifying potential vulnerabilities and acting to mitigate them before and after breach will become more complex and more resource-intensive. The tradeoff is that the IOT will bring increased convenience and functionality for both business and consumers; but it will come at a price.

Cloud computing also cuts two ways. On the one hand, it opens up avenues for a wider range of enterprises to obtain services for cybersecurity and other purposes. On the other hand, the cloud also changes the landscape in which adversaries operate by providing a tempting target, rich in assets for attack. Whereas potential targets may currently be more dispersed, the cloud concentrates them to a greater degree—although the owners and operators of Internet-based cloud technologies and services may be comparatively well-placed to defend the valuable constellations of data and other assets that are effectively entrusted to them. Another trend, in the form of increasingly distributed enterprises, also alters the cybersecurity ecosystem for network defenders and network attackers at once. Here again, the evolution in practice brings with it new challenges for the in-house security practitioner, including "more places where it [data] must be protected."[129]

As technology continues to change so too will the capabilities—and accompanying intentions—of threat actors. However, the counterforces they face will not remain static either: new elements will enter the fray, and the capacities and roles of existing actors will develop as well. For example, what is the role for state and local governments when it comes to active defense? Just as these authorities have become ever-more involved over time in matters of cybersecurity more generally, one might expect state and local officials to participate (eventually) in the domain of active defense in particular.

Another important question for the future is: how will international norms develop in this area? The answer depends upon individual actors (state and non-state) as well as the totality of their conduct. These practices and the statements made in support of—or in protest to—them will constitute evidence of emerging global parameters of acceptable behavior. Formal international instruments such as global treaties are, admittedly, generally difficult to draft and bring into force given the wide variety of competing viewpoints that must be accommodated and reconciled. Therefore, it may prove constructive in the shorter term to work towards a more informal international understanding of what should be the core body of

principles governing active defense—perhaps in the form of a voluntary code of conduct. In contrast to a multilateral (interstate official) agreement such a tool is by definition non-binding, though it could still reflect the consensus opinion of a range of key participants in active defense worldwide, and thereby serve as a building block for the creation of more embedded international norms in the future.

The Center for Cyber and Homeland Security and the Task Force co-chairs look forward to to continuing to work on these and related issues as they continue to engage on these and associated cyber policy matters in the years ahead.

Appendix I: Additional Views of Nuala O'Connor

This report is a necessary contribution to the important conversation around the appropriate cybersecurity defensive measures that companies can take to respond to and prevent attacks. The George Washington Center for Cyber and Homeland Security and the members of the Task Force are to be commended for their efforts to further a constructive dialogue and contribute to the scholarship on these issues. If policy makers draw only one lesson from the report, it should be that the "gray zone" between lawful and unlawful defensive measures must shrink. The current level of ambiguity between lawful and unlawful defensive measures poorly serves corporate, privacy, data security, national security, and law enforcement interests. I write separately to express my concern that the report advocates a more aggressive posture than I believe appropriate, and does not give adequate weight to security and privacy risks of some of the techniques it favors.

I appreciate the willingness of the Task Force, and in particular, my colleague Frank Cilluffo, to consider and provide space in the dialogue for these views. I also want to recognize our team at the Center for Democracy & Technology—especially Chris Calabrese, Joseph Lorenzo Hall, Greg Nojeim and Gabe Rottman—for their insights and contribution to these comments.

The report draws a line between "active defense" measures that Congress and the executive branch should make lawful or consider lawful, and "hacking back" which would remain unlawful. I believe that the line between them, consistent with the line drawn in the Computer Fraud and Abuse Act (CFAA) and the Cybersecurity Information Sharing Act, should be the act of gaining unauthorized access to another's computer or network, as recognized by the US Department of Justice (DOJ) and the US Department of Homeland Security.[130] The unauthorized access bar should be raised by amending the CFAA to add a requirement that to be unlawful, the act of gaining unauthorized access must involve circumventing a technical access control. This would ensure that mere "terms of service" violations do not trigger CFAA civil and criminal liability.

Instead, the report invites companies to engage in active defense measures that involve gaining unauthorized access to another's computer or network, so long as the entity engaging in this activity does not do so with intent to cause harm. For example the report discusses the use of "dye packs" and "white hat ransomware"—both of which involve gaining unauthorized access to another's computer or network and placing malware on those systems—as more aggressive active defense measures that might become lawful based on considerations like whether they were conducted in conjunction with the government and the intent of the actor.

I believe these types of measures should remain unlawful. Intent can be difficult to measure, particularly when on the receiving end of an effort to gain access. Because attacks are often launched through the computers of innocent people, and because attack attribution is at best an inexact science, the risk of harm in these methods that gain unauthorized access can fall upon other victims of the attack and on innocent bystanders.

The risks of collateral damage to innocent internet users, to data security, and to national security that can result from overly aggressive defensive efforts needs to be better accounted for. There are examples of defensive measures that had unintended consequences, and lessons can be learned from those cases. For example, Microsoft's efforts to take down two botnets associated with the dynamic DNS service offered by no-ip.com had the effect of temporarily denying DNS service to 5 million people, effectively causing 99.8%

collateral damage to users of no-ip's service, and causing those domains to be completely inaccessible to their users and customers for two days.[131] Instead, as an example of active defense measures companies could take, the report mentions Google's response to operation Aurora. Based on existing evidence it seems likely that response involved gaining unauthorized access to computers in Taiwan that were believed to be under the control of entities in China and inspecting data on those computers—serious conduct with national security and foreign law implications that the must be more thoroughly addressed.

Some of the more aggressive defensive measures the report mentions, if permitted at all, should be engaged in by law enforcement or under the direction of a law enforcement agency. "Coordination" with law enforcement may not be enough. Moreover, the report only briefly dwells on the risks of government hacking or of the myriad controls that should be imposed to prevent or ameliorate harm. Just a few of the unanswered questions include: What kind of court order would be required to permit such government conduct? How would it constrain that conduct, and when? How and when would the government give notice to the targets of these defensive measures, when those targets will invariably perceive this conduct as attacks? Further, since, as the report does note, government notice in these contexts could be spoofed and, if the conduct becomes normalized, could become an additional vector of attack, what steps will be taken to authenticate the sender or prevent such abuse?

There is also an ongoing and active debate regarding the scope of law enforcement hacking in criminal investigations under a revised Rule 41—the authority DOJ would likely use in some of the contemplated active defense scenarios. Those actions are certain to result in overbroad searches and possibly damage to the computers of many innocent people who have already been the victims of hacking.[132]

When it comes to risky defensive conduct that may cross the line and be unlawful, the report makes two observations that give me pause. First, that some cybersecurity firms might be given a license to operate as agents of the federal government and engage in conduct that would be unlawful for other private parties. Second, that the Department of Justice forbear prosecution of companies that engage in unlawful active defense measures. The first may be unwise and would be difficult to implement. The report does not address any limits and controls under which the licensed firm would operate, or the qualifications that would be required of licensees, or how they themselves and consequences of their actions will be overseen. The second—possible DOJ forbearance—would grow rather than shrink "the gray zone" of permissible conduct. And, in some cases, forbearance may be appropriate, but in instances where an entity actually circumvents a technical access control, prosecution may indeed be warranted. A call for DOJ forbearance must better account for the computer crimes laws of other countries that would be implicated in many active defense scenarios where the affected system is located in another country.

I recognize the Task Force's efforts to accommodate many of my concerns. Ultimately though, I would have preferred a more moderate approach. As this discussion progresses, I urge greater outreach to privacy and civil liberties groups beyond the experts whose views were sought. Hopefully the report will put active defense higher on the agenda of more stakeholders. We look forward to continuing to participate in this discourse, and to ensuring that active defense measures include protections for civil liberties while not undermining the integrity of the architecture of computer and networked systems.

Appendix II: Legal Analysis
Courtesy of Covington & Burling, LLP

I. Most Relevant U.S. Statutes

A. Computer Fraud and Abuse Act (18 U.S.C. § 1030 *et seq.*)

1. Main Restrictions—it is illegal for anyone who:

a) Accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer;

b) Knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

c) Intentionally access a protected computer without authorization, and as a result of such conduct, recklessly cause damage; or

d) Intentionally access a protected computer without authorization, and as a result of such conduct, cause damage and loss.

2. Practical Effect/Examples

a) Most of the aggressive cyber defense measures (and perhaps some of the more intermediate) likely would violate this law.

(1) For example, any measure that would recover, erase, or alter stolen data or send malware to disrupt an attack likely would require unauthorized access to a computer and would obtain data from or cause damage to that computer.

(2) Less clear are intermediate measures such as observation and monitoring outside a company's network or beaconing. While these may require access to a computer, they may not involve obtaining information or causing damage.

b) The statute has been interpreted very broadly (e.g., a protected computer is any computer connected to the internet, *United States v. Trotter*, 478 F.3d 918 (8th Cir. 2007)) but there is also some ambiguity about the meaning of "authorization" and therefore the meaning of "without authorization" or "exceeds authorized access." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132-33 (9th Cir. 2009), *United States v. Valle*, No. 14-2710 et al. (2d. Cir. 2015).

(1) Nevertheless, active cyber defense measures that involve accessing an attacker's computer or network to obtain or destroy data likely would qualify as "without authorization" or "exceeds authorized access."

3. Potential Amendments?

a) Potential carve out for self-defense measures or self-help privileges. *See* Shane Huang, *Proposing A Self-Help Privilege for Victims of Cyber Attacks*, 82 Geo. Wash. L. Rev. 1229, 1245 (2014).

B. Electronic Communications Privacy Act ("ECPA")—The Wiretap Act (18 U.S.C. § 2510 *et seq.*)

1. Main Restrictions—It is illegal for anyone to:

a) Intentionally or purposefully intercept (or endeavor to intercept), disclose or use the contents of any wire, oral, or electronic communication;

b) Intentionally or purposefully use (or endeavor to use) a device to intercept oral communication.

c) A "device" is any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than a telephone or telegraphy equipment given to the user by a provider of wire or electronic communication and used in the ordinary course of business, or a hearing aid or similar device.

2. Practical Effect/Examples

a) While most of the analysis centers on the CFAA, some cyber defense tactics may also violate the Wiretap Act. For example, practices such as sinkholing may violate the Wiretap Act to the extent that intercepting malicious traffic would be considered an intercept of an electronic communication. See Sean L. Harrington, *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?*, 20 Rich. J.L. & Tech. 17 (2014).

3. Potential Amendments?

a) The Wiretap Act has an exception that allows law enforcement officials to monitor activity of hackers when certain limited criteria are met (including when the owner or operator of the network authorizes the interception and when there is a lawful investigation). *See* 18 U.S.C. § 2511(2)(i)(I)-(IV); *see also* Harrington, 20 Rich. J.L. & Tech. 12. There could be some potential to expand on this exception or add to the criteria circumstances involving cyber defense or stolen data.

C. Electronic Communications Privacy Act ("ECPA")—Pen Register/Trap and Trace (18 U.S.C. § 3121-27)

1. Main Restrictions—prohibits anyone from:

a) Installing a pen register or trap and trace device without obtaining a court order

b) A "pen register" is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication…" 18 U.S.C. § 3127(3).

c) A "trap and trace device" is a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication…" 18 U.S.C. § 3127(4).

2. Practical Effect/Examples

a) Prohibition on "trap and trace" devices may apply to intermediate cyber defense measures such as honeypots or sinkholes that operate to capture incoming data and identify the source of intrusion or attack.

b) Emphasis here is really demonstrating the role that the government would play in cyber defense measures, i.e., the need to obtain a court order to install a pen register or trap and trace device.

II. Common Law Theories

A. Trespass to Chattels

1. Elements

a) Trespass to chattels is "intentionally…dispossessing another of the chattel, or using or intermeddling with a chattel in the possession of another." Restatement (Second) of Torts § 217.

b) Accordingly, one needs to prove (1) intent, (2) interference with the chattel, and (3) actual harm. *See* T. Luis de Guzman, *Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges*, 59 Catholic U L Rev. 527 (2010).

2. Examples

a) Courts have found that spam email interfered with an email server enough to amount to an action for trespass to chattels. *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021 (S.D. Ohio 1997); *see also* Huang, 82 Geo. Wash. L. Rev. at 1242.

b) A trespass to chattels action could also arise due to unwanted computer access. *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393 (2d Cir. 2004) (finding that continued, automated behavior consumed capacity of Register.com's computer system and impaired their quality and value); *see also* Huang, 82 Geo. Wash. L. Rev. at 1242, 43.

c) Ultimately, trespass to chattels may require repeated access that causes some harm to computer performance. Huang, 82 Geo. Wash. L. Rev. at 1242, 43.

d) It also can be difficult to identify one individual attacker to sue. *See* Jay P. Kesan & Carol M. Hayes, Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace, 25 Harv. J.L. & Tech. 429, 497-98 (2012).

3. Practical Effect

a) Under certain circumstances, one can interfere with another's chattels to defend his or her own chattels. *See* de Guzman, 59 Catholic U L Rev. at 542. The Restatement (Second) of Torts recognizes this privilege: "one is privileged to commit an act which would otherwise be a trespass to a chattel or a conversion if the act is, or is reasonably believed to be, necessary to protect the actor's land or chattels or his possession of them, and the harm inflicted is not unreasonable as compared with the harm threatened." Restatement (Second) of Torts § 260(1).

b) A company might be able to use this concept to shield itself from liability for cyber defense measures. However, such measures could include other actions that could be found tortious, or even in violation of the CFAA. *See* de Guzman, 59 Catholic U L Rev. at 542.

B. Negligence

1. Elements

a) Duty of care, breach, causation, and damages.

2. Practical Effect/Examples

a) Commentators have proposed holding intermediary parties responsible for failure to secure their systems. Kesan & Hayes, 25 Harv. J.L. & Tech. at 498; see de Guzman, 59 Catholic U L Rev. at 548.

b) For example, a "zombie" computer owner, ISP, or software manufacturer could all be held liable for failing to safeguard their own devices which in turn were used to launch an attack on the ultimate victim. *See* Kesan & Hayes, 25 Harv. J.L. & Tech. at 498.

3. Limitations

a) It could be challenging to establish a duty of care and show causation in many cases. *See* Kesan & Hayes, 25 Harv. J.L. & Tech. at 499. ISPs and other service providers could avoid liability through contractual terms. *See id.* at 499-500.

b) No recourse for companies to retrieve stolen data or to fix damages to network or computer caused by attack.

III. International Law

A. No Overarching International Law for Private Actors

1. There is no overarching international law that specifically addresses active cyber defense by private actors. *See* Paul Rosenzweig, International Law and Private Actor Active Cyber Defensive Measures, 50 Stan. J. Int' L. 103 (2014).

B. International Law Focuses on Nation-States

1. Most of the applicable international law focuses on the actions of nation-states

2. This includes the UN Charter and other laws governing nations' right to self-defense. *See* Michael N. Schmitt, In Defense of Due Diligence in Cyberspace, 125 Yale L. J. (2015); *see also* Tallinn Manual.

C. Countries' Own Domestic Laws

1. Some countries have enacted laws that address active cyber defense. For example:

   a) Germany has made hacking back illegal (although anecdotal evidence suggests that private entities in Germany engage in this tactic anyway). Rosenzweig, 50 Stan. J. Int' L. 103

   b) Netherlands proposed law allowing enforcement officials to hack back internationally. *Id.*

   c) Israeli Defense Forces reserve right to use offensive cyber operations but law is silent on ability of private actors to do the same. *Id.*

2. Private companies may be liable for active cyber defense actions that are taken against a computer or a network in a country with a domestic law prohibiting such actions. *Id.* (hypothesizing that "when a private sector hack back has collateral effects in an allied country . . . we can imagine that U.S. legal authorities would generally honor an appropriately couched extradition request from the affected nation.").

D. Analogous International Laws

1. Certain laws such as the Budapest Convention, Rome Statute, International Criminal Tribunal provide opportunities to analyze whether the self-defense provisions under these laws could be extrapolated to cyber activities. *Id.* Most allow some sort of self-defense, even if it is limited.

2. Law of piracy would allow for self-defense but not active pursuit (which would be left only to states and only within their own territorial waters). *Id.*

3. Letters of marque would suggest a state's explicit acceptance and/or direction of action to retaliate against malicious cyber activity. *Id.*

Appendix III: Global Perspectives on Active Defense

IN A GLOBALIZED WORLD, corporations, threat actors, and computer networks are unrestricted by political boundaries. While this report's focus is on private sector active defense in the context of U.S. policy and law, it is worthwhile to briefly summarize the active defense "climates" in four foreign countries that are relevant in the realm of cybersecurity. As is seen in the following examples, every country creates unique architectures to deal with cyber threats, enacts different computer trespass laws, and socializes different cybersecurity norms. These factors all influence the level to which countries consider implementing policies conducive to private sector active defense. The following section details the active defense climates of the United Kingdom, France, Estonia, and Israel.

The United Kingdom

The 2010 UK National Security Strategy characterized cyber-attacks as a "Tier One" ("highest priority") threat and, since then, the government has been working with the private sector to share threat-related information.[133] Against this background, the UK security and intelligence agency, Government Communications Headquarters (GCHQ), has been helping to build awareness of—and resilience to—the cyber threat in the critical financial services sector, by supporting efforts to test, train, and exercise capabilities in this area.[134] The country's new National Cyber Security Centre (NCSC) is intended to reinforce and expand the effort to inform and support against cyber threats to the business community and beyond.[135] Hackers have hit Britain's biggest banks—from HSBC[136] to Standard Chartered[137] to Barclay's[138]—repeatedly in recent years. Analysts have emphasized the major banks' vulnerabilities, introduced by "their complex and ageing web of overlapping computer systems."[139]

At last year's World Economic Forum in Davos, active defense was the subject of vigorous discussion among global bankers—with signs of a "transatlantic split"—as some European executives conceived of both threat and potential response in considerably less "aggressive" terms than their American counterparts.[140] Eighteen months later, however, it is the unfolding ramifications of the UK decision to leave the European Union ("Brexit") that are top of mind. That said, the framework that prevails in the United Kingdom in regard to active defense by the private sector against cyber threats is comparable to that which exists in the United States. Nevertheless, there is ambiguity at the tactical level, with some UK counsel arguing that certain measures to amass attacker-related information are permissible: *e.g.,* injecting code to collect intelligence (beyond just an IP address); and yet others considering such actions to be outside legal bounds.[141]

France

The larger context of a company's position in the marketplace shapes the need for—and manner of implementation of—private sector active defense against cyber threats. In the case of France, government ownership (even if partial) persists in diverse domains from banking to energy to telecommunications. This stands in contrast to the United States and the United Kingdom, where privatization levels are much more extensive. Against the background of this greater blurring of the line between the state and enterprise, France has engaged actively in industrial espionage (despite protestations to the contrary)[142], to the benefit of French economic interests. At the same time, French companies have been targeted. Yet, according to the former head of DCRI (the predecessor to the French internal intelligence agency DGSI):

"Companies rarely admit security breaches or seek the help of the state."[143]

Under current French law, however, operators of "essential services" are required to report cyber breaches[144]; and the European Union framework now obliges the same.[145] In 2015, France also introduced legislation that explicitly empowers the country's intelligence entities to conduct surveillance for specified areas and purposes—including "essential industrial and scientific interests."[146] A new dedicated entity for strategic intelligence and economic security stood up earlier this year.[147] In addition, legislation intended to frustrate threat actors who use encryption continues to advance domestically[148]; and at the international level, France is working in parallel to spur a global effort to achieve similar effect.[149] Increasingly, therefore, French officials are focusing on the points of intersection between economic security and national security.

Estonia[150]

In order to protect its rapidly developing e-government infrastructure, Estonia began to promote cybersecurity through national policy in the early 2000's. It adopted its first national cybersecurity strategy in 2008[151] after the well-known DDoS attacks of 2007.[152] Following several years of active institutional development, including the establishment of the NATO Cyber Defence Center in Tallinn, the incorporation of the Estonian Information Systems Authority, and the creation of a national cyber security council, Estonia became one of a few countries to adopt a second national strategy in 2014.[153]

Despite these developments, Estonia has no overarching national legal framework that governs cybersecurity and cyber defense. This is not to say that Estonian law has nothing to say about cyber. The Penal Code defines certain computer crimes, including unauthorized access to computer systems, and the Emergency Act governs organizational and governmental cybersecurity. Estonia is also a signatory to the Council of Europe's Convention on Cybercrime[154] and is subject to EU directives, such as the recent directive on security of network and information systems.

The topic of active defense is rarely an explicit part of Estonian public discourse on cybersecurity, especially within the private sector. However, public and private entities engage in certain activities that fall under its remit. Among other initiatives, Estonian intelligence agencies, the national CERT, and the Information System Authority share information among themselves, with the private sector, and with international counterparts to facilitate rapid response to emerging cyber threats and improve critical infrastructure cybersecurity. Government agencies also conduct penetration tests of critical infrastructure companies, hold regular public-private cyber defense exercises, and collaborate with international partners in takedown operations.[155]

Ultimately, there is no discernible momentum in Estonia for policy changes in the field of private sector active defense, nor are there particularly loud calls for such changes from company executives. This may be due to the lack of an overarching legal framework for cyber security in Estonia—the development of which is a priority under the most recent national cybersecurity strategy—or by the fact that private sector leaders do not publicly discuss active defense measures. However, it is more likely that Estonia's small size and intensive public-private cooperation provide its private sector entities with greater access to governmental attention and resources, an advantage that may be unavailable to private entities in larger European or North American countries. Barring major political or external pressure, this arrangement is unlikely to change in the near future.

Israel

Out of necessity, Israel has developed advanced cybersecurity capabilities that include Unit 8200 of the Israel Defense Forces (IDF).[156] The country's private sector too, has had to develop operational strategies to counter sustained cyber-attacks and industrial espionage. Notably, Israel's cybersecurity industry is a major player in the global market, and continues to attract capital and investors.[157] The sector also benefits from the skills and experience that former mem-

bers of IDF Unit 8200 have brought to Israel's vibrant "tech startup" community.[158]

The tenor of the national dialogue in Israel, spanning both the public and private sectors, is supportive of a forward-leaning and robust posture on matters of cybersecurity.[159] The country's legal framework in this area is comparatively relaxed relative to that of the United States.[160] (Indeed, anecdotal evidence suggests that U.S. firms wishing to take a more active posture on cybersecurity have contracted with Israeli firms in order to circumvent U.S. strictures in this area).[161]

From a government standpoint, Israel's National Cyber Bureau (NCB) coordinates the country's cybersecurity initiatives while supporting the private sector. As part of the Prime Minister's Office, the NCB funds research and development, and works to improve public-private sector collaboration in accordance with the government's "Digital Israel" initiative.[162] Furthermore, since its establishment in 2002, Israel's National Information Security Authority has directly advised owners of critical infrastructure situated in the private sector, on cybersecurity issues.[163]

Appendix IV: Glossary of Terms

Term	Definition and Source
Advanced Persistent Threat (APT)	"An adversary that possesses sophisticated levels of expertise and significant resources which allow it to achieve its objectives using multiple attack vectors. (NIST SP 800-61)." "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives." SP 800-39. http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf
Anti-malware	"A technology widely used to prevent, detect and remove many categories of malware, including computer viruses, worms, Trojans, keyloggers, malicious browser plug-ins, adware and spyware." http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf
Beaconing	"A way to enhance electronic files to allow for awareness of whether protected information has left an authorized network and can potentially identify the location of files in the event they are stolen.'" Sean L. Harrington, Cyber Security Active Defense: Playing with Fire or Sound Risk Management?, 20 Rich. J.L. & Tech. 1, 9 (2014) (citing Comm'n on the Theft of Am. Intellectual prop., The IP Commission Report 81 (2013), available at http://ipcommission.org/report/IP_Commission_Report_052213.pdf).

Term	Definition and Source
Blacklisting	"The process of the system invalidating a user ID based on the user's inappropriate actions. A blacklisted ID cannot be used to log on to the system, even with the correct authenticator. Blackslisting and lifiting of a blacklisting are both security-relevant events. Blacklisting also applies to blocks placed against IP addresses to prevent inappropriate or unauthorized use of Internet resources." CNSSI-4009."A list of email senders who have previously sent spam to a user." SP 800-114. "A list of discrete entities, such as hosts or applications, that have been previously determined to be associated with malicious activity." SP 800-94. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
Botnet	"A term derived from 'robot network;' is a large automated and distributed network of previously compromised computers that can be simultaneously controlled to launch large-scale attacks such as a denial-of-service attack on selected victims." http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf
Botnet takedown	"Actions taken to identify and disrupt a botnet's command and control infrastructure." http://timreview.ca/article/862
Challenge and Reply Authentication	"A prearranged procedure in which a subject requests authentication of another and the latter establishes validity with a correct reply." CNSSI-4009 http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
Communications deception	"Deliberate transmission, retransmission, or alteration of communications to mislead an adversary's interpretation of the communications." CNSSI-4009. "Alteration or simulation of friendly telecommunications for the purpose of deception." CNSSI-4009. "Introduction of deceptive messages or signals into an adversary's telecommunication signals." CNSSI-4009. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
Computer Network Attack	"Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." CNSSI-4009. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
Computer Network Defense	"Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities." CNSSI-4009. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Term	Definition and Source
Computer Network Exploitation	"Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks." CNSSI-4009. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
Critical infrastructure	"System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. [Critical Infrastructures Protection Act of 2001, 42 U.S.C. 5195c(e)] CNSSI-4009. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
Cyber attack	"An attack that alters a system or data." CNSSI-4009. "An attack on the authentication protocol where the Attacker transmits data to the Claimant, Credential Service Provider, Verifier, or Relying Party. Examples of active attacks include man-in-the-middle, impersonation, and session hijacking." SP 800-63. "An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity." SP 800-32. "Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself." CNSSI-4009. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
Cyber deterrence by denial	"Reducing the incentive of potential adversaries to use cyber capabilities against the United States by persuading them that the United States can deny their objectives . . . The President has at his disposal a number of tools to carry out deterrence by denial. These include a range of policies, regulations, and voluntary standards aimed at increasing the security and resiliency of U.S. government and private sector computer systems. They also include incident response capabilities and certain law enforcement authorities, such as those used by the Department of Justice to take down criminal botnets. They include cyber threat information sharing mechanisms, as well as public-private partnerships." "efforts . . . to persuade adversaries that the United States can thwart malicious cyber activity, thereby reducing the incentive to conduct such activities. To make these deterrence efforts credible, we must deploy strong defenses and architect resilient systems that recover quickly from attacks or other disruptions." *Continued on the next page*

Term	Definition and Source
Cyber deterrence by denial (continued)	"Pursuing defense, resiliency, and reconstitution initiatives to provide critical networks with a greater capability to prevent or minimize the impact of cyber attacks or other malicious activity, and reconstitute rapidly if attacks succeed. Building strong partnerships with the private sector to promote cybersecurity best practices; assist in building public confidence in cybersecurity measures; and lend credibility to national efforts to increase network resiliency." Department of State International Cyberspace Policy Strategy, Public Law 114-113, Division N, Title IV, §402 (March 2016), https://www.state.gov/documents/organization/255732.pdf.
Cyber espionage	"Activities conducted in the name of security, business, politics, or technology to find information that ought to remain secret. It is not inherently military." http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf
Cyber Infrastructure	"Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., supervisory control and data acquisition-SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure." NISTIR 7628. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
Cybersecurity	"The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems." http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf
Cyberspace	"A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." CNSSI-4009. http://www.globaltimes.cn/content/1010409.shtml

Term	Definition and Source
Dark Net	"A collection of websites that are publicly visible but hide the Internet Protocol addresses of the servers that run these sites." "The Dark Web relies on darknets or networks that are made between trusted peers. Examples of Dark Web systems include TOR, Freenet, or the Invisible Internet Project (I2P). Vincenzo Ciancaglini et al., Below the Surface: Exploring the Deep Web, TrendLabs Research Paper, TrendMicro (2016) https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf.
Deep Web	"Any Internet content that, for various reasons, can't be or isn't indexed by search engines like Google. This definition thus includes dynamic web pages, blocked sites (like those that ask you to answer a CAPTCHA to access), unlinked sites, private sites (like those that require login credentials), non-HTML/-contextual/-scripted content), and limited-access networks." Vincenzo Ciancaglini et al., Below the Surface: Exploring the Deep Web, TrendLabs Research Paper, TrendMicro (2016) https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf.
Denial of Service (DoS)	"The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.). CNSSI-4009. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
Distributed Denial of Service Attack (DDoS)	"A Denial of Service technique that uses numerous hosts to perform the attack." CNSSI-4009. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
Dye pack	See beaconing. In the cybersecurity context, the terms beacon and dye pack are often used interchangeably. However, with the term's physical namesake being the dye packs used to identify bank robbers, the cybersecurity tool sometimes takes on a more aggressive connotation. Where, in bank robberies, dye packs explode and contaminate the stolen money and their environment with a recognizable dye, cyber dye packs are often thought to not only be able to collect information on a hacker's computer (similar to a beacon) but also to be able to have a destructive impact on their surrounding environment.

Term	Definition and Source
Firewall	"A system or combination of systems that enforces a boundary between two or more networks, typically forming a barrier between a secure and an open environment such as the Internet." "A gateway that limits access between networks in accordance with local security policy." SP 800-32. "A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy." CNSSI-4009. "A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures." SP 800-41. http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf; http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
Honeypot	"A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner such that their actions do not affect production systems." "A system (e.g., a Web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders and has no authorized users other than its administrators. CNSSI-4009. http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf; http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
Information Sharing and Analysis Center	"ISACs help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency . . . ISACs are trusted entites established by critical infrastructure owners and operators to foster information sharing and best practices about physical and cyber threats and mitigation. About ISACs, National Council of ISACs (Accessed Oct. 14, 2016), http://www.isaccouncil.org.
Patching	"Fixes to software programming errors and vulnerabilities." The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs." CNSSI-4009. http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf; http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
Quarantine	"Store files containing malware in isolation for future disinfection or examination." SP 800-69. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Term	Definition and Source
Ransomware	"Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively called crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key." Ransomware, TrendMicro (accessed Oct. 10, 2016), http://www.trendmicro.com/vinfo/us/security/definition/ransomware.
Remote Access Tools (RATs)	Tools that allow either authorized or unauthorized remote access, i.e., "access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (e.g., the Internet)." SP 800-53. "Access by users (or information systems) communicating external to an information system security perimeter." SP 800-17. "The ability for an organization's users to access its nonpublic computing resources from external locations other than the organization's facilities." SP 800-46. "Access to an organization's nonpublic information system by an authorized user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). CNSSI-4009. http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf
Sinkholing	"A mechanism aimed at protecting users by intercepting DNS requests attempting to connect to known malicious or unwanted domains and returning a false, or rather controlled IP address. The controlled IP address points to a sinkhole server defined by the DNS sinkhole administrator. This technique can be used to prevent hosts from connecting to or communicating with known malicious destinations such as a botnet C&C server." DNS Sinkhole, European Union Agency for Network and Information Security (accessed Oct. 14, 2016), https://www.enisa.europa.eu/topics/national-csirt-network/glossary/dns-sinkhole.
Social engineering	"An attack based on deceiving users or administrators at the target site into revealing confidential or sensitive information." http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf
Spyware	"Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code." SP 800-53, CNSSI-4009. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Term	Definition and Source
Tarpits	"Allowing a tarpitted port to accept any incoming TCP connection. When data transfer begins to occur, the TCP window size is set to zero, so no data can be transferred within the session. The connection is then held open, and any requests by the remote side to close the session are ignored. This means that the attacker must wait for the connection to timeout in order to disconnect." http://csrc.nist.gov/cyberframework/framework_comments/20131213_charles_alsup_insa_part3.pdf
White hat	"White hats are security researchers or hackers who, when they discover a vulnerability in software, notify the vendor so that the hole can be patched." Kim Zetter, Hacker Lexicon: What are White Hat, Gray Hat, and Black Hat Hackers?, Wired (April 13, 2016), http://docs.house.gov/meetings/IF/IF17/20150324/103226/HHRG-114-IF17-Wstate-SchoolerR-20150324.pdf.
Whitelisting	"A list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organization and/or information system." SP 800-128. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
Zero-day exploits	"A vulnerability that is exploited before the software creator/vendor is even aware of its existence." http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf

Notes

1. Chase Gunter, "*Cyberwar keeps CIA's Brennan Up at Night*," *FCW*, February 16, 2016, https://fcw.com/articles/2016/02/16/brennan-interview-recap.aspx; U.S. Department of Defense, "The Department of Defense Cyber Strategy" April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf; Steve Morgan, "J.P. Morgan, Bank of America, Citibank, and Wells Fargo Spending $1.5 billion to Battle Cyber Crime," *Forbes*, December 13, 2015, http://www.forbes.com/sites/stevemorgan/2015/12/13/j-p-morgan-boa-citi-and-wells-spending-1-5-billion-to-battle-cyber-crime/#5688f5da1112; Mary Jo White, "Opening Statement at SEC Roundtable on Cybersecurity," U.S. Securities and Exchange Commission, March 26, 2014, http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541286468.

2. David Burg, "Concern Over Cyber Threats has CEOs Warming to Government Collaboration," *PricewaterhouseCoopers* (2015), http://www.pwc.com/us/en/ceo-survey-2015/secure-assets.html.

3. Jessica Silver-Greenberg, Matthew Goldstein, and Nicole Perlroth, "JPMorgan Chase Hacking Affects 76 Million Households," *New York Times,* October 2, 2014, http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_r=0; Fran Howarth, "US State Department Hack has Major Security Implications," *Security Intelligence* (2015), https://securityintelligence.com/us-state-department-hack-has-major-security-implications/; Elias Groll, "The Same Russian Hackers Hit the DNC and DCCC, Security Firms Say," *Foreign Policy,* August 1, 2016, http://foreignpolicy.com/2016/08/01/the-same-russian-hackers-hit-the-dnc-and-the-dccc-security-firms-say/; Devlin Barrett and Katy Burne, "Now it's Three: Ecuador Bank Hacked via Swift," *Wall Street Journal*, May 19, 2016, http://www.wsj.com/articles/lawsuit-claims-another-global-banking-hack-1463695820.

4. Justin McCarthy, "Americans Cite Cyberterrorism Among Top Three Threats to US," *Gallup* (2016), http://www.gallup.com/poll/189161/americans-cite-cyberterrorism-among-top-three-threats.aspx. The percentage of Americans responding that Cyberterrorism was a critical threat (73%) was the third highest of all threats included in the poll and received the most bipartisan agreement.

5. Michael Chertoff and Frank Cilluffo, "A Strategy of Cyber Deterrence," *Choosing to Lead: American Foreign Policy for a Disordered World,* John Hay Initiative (2015), http://www.choosingtolead.net/a-strategy-of-cyber-deterrence.

6. "World's Biggest Data Breaches: Selected Losses Greater than 30,000 Records," *Information is Beautiful*, October 15th, 2016 http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

7. Frank J. Cilluffo, "Testimony on Emerging Cyber Threats to the United States," in *U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies*, (2016) http://docs.house.gov/meetings/HM/HM08/20160225/104505/HHRG-114-HM08-Wstate-CilluffoF-20160225.pdf.

8. Tim Maurer, "Cyber Proxies and the Crisis in the Ukraine," *NATO CCD COE Publications* (2015), https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Maurer_09.pdf; Owen Matthews, "Russia's Greatest Weapon may be its Hackers," *Newsweek,* May 15, 2015, http://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html.

9. *Worldwide Threat Assessment of the US Intelligence Community: Statement for the Senate Armed Services Committee* (2016), statement of James R. Clapper, https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.

10. Frank J. Cilluffo, "Testimony on Emerging Cyber Threats to the United States."

11. Lorenzo Vidino and Seamus Hughes, "ISIS in America: From Retweets to Raqqa," the George Washington University Program on Extremism (2015), https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/ISIS%20in%20America%20-%20Full%20Report.pdf; Rachel Weiner and Ellen Nakashima, "Hacker Admits he Gave Military Members' Data to the Islamic State," *The Washington Post* (2016), https://www.washingtonpost.com/local/public-safety/hacker-admits-he-gave-military-members-data-to-isis/2016/06/15/975deeb4-330b-11e6-8758-d58e76e11b12_story.html.

12. Robert Siciliano, "7 Types of Hackers and their Motivations," *McAfee blog* (2011), https://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/

13. U.S. Department of Defense, "The Department of Defense Cyber Strategy."

14. *United States of America vs. Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Ahmadzadegan, Omid Ghaffarinia, Sina Keissar, and Nader Saedi*, (Sealed Indictment) U.S. Attorney's Office S.D.N.Y. (2016), https://www.justice.gov/opa/file/834996/download.

15. Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," *SANS Industrial Control System and the Electricity Information Sharing and Analysis Center* (2016), https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

16. Josh Rogin, "NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history,'" *Foreign Policy,* July 9, 2012, http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history.

17. https://www.justice.gov/opa/pr/russian-cyber-criminal-convicted-38-counts-related-hacking-businesses-and-stealing-more-two

18. "The World if Financial Systems were Hacked," *The Economist*, June 16, 2016, http://worldif.economist.com/article/12136/joker-pack.

19. Dennis Blair and John M. Huntsman Jr., "The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property," *The National Bureau of Asian Research* (2013), http://www.ipcommission.org/report/ip_commission_report_052213.pdf.

20. Roger C. Molander, Peter A. Wilson, and Robert H. Anderson, "U.S. Strategic Vulnerabilities: Threats Against Society," *Strategic Appraisal*, *RAND* (1999), https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1016/MR1016.chap9.pdf.

21. Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel JG Van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. "Measuring the cost of cybercrime." *The Economics of Information Security and Privacy*, Springer Berlin Heidelberg (2013), 265-300, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

22. Eric Cohen and Davide di Gennaro, "Cybersecurity and Payment Fraud: The Challenge for Treasury," *PricewaterhouseCoopers* (2015), http://www.pwc.com/us/en/risk-management/publications/cybersecurity-and-payment-fraud-the-challenge-for-treasury.html.

23. "Operation Blockbuster Unraveling the Long Thread of the Sony Attack," *Novetta* (2016) https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf; Nicole Perlroth, "Yahoo Says Hackers Stole Data on 500 Million Users in 2014," *The New York Times,* September 23, 2016, http://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html; Ellen Nakashima, "Cyber Researchers Confirm Russian Government Hack of Democratic National Committee," *The Washington Post,* June 20, 2016, https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html.

24. Torri Piper, "An Uneven Playing Field: The Advantages of the Cyber Criminal vs. Law Enforcement—and Some Practical Suggestions," *SANS Institute* (2002), https://www.sans.org/reading-room/whitepapers/legal/uneven-playing-field-advantages-cyber-criminal-vs-law-enforcement-and-practica-115.

25. Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." *Leading Issues in Information Warfare & Security Research* 1 (2011): 80, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.

26. Dimitar Kostadinov, "The Cyber Exploitation Life Cycle," *Infosec Institute* (2013), http://resources.infosecinstitute.com/the-cyber-exploitation-life-cycle.

27. Giora Engel, "Deconstructing the Cyber Kill Chain," *Dark Reading* (2014), http://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542.

28. Amol Sarwate, "2016 State of Vulnerability Exploits," Paper presented at the RSA Conference 2016, San Francisco, California, February 29-March 4, 2016, https://www.rsaconference.com/writable/presentations/file_upload/spo2-t09-2016-state-of-_vulnerability-exploits_v2.pdf.

29. Press Release, Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence

on Election Security." Office of the Director of National Intelligence, October 7, 2016. https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement

30. Robert Gilpin, *War and Change in World Politics.* Cambridge University Press (1983).

31. While law enforcement organizations are also confronted with the challenges of limited resources when combating traditional crimes, they benefit from the ability to periodically and visibly "flex" their enforcement muscles in ways that remind threat actors that their actions will not go unnoticed or unchecked. Such visible deterrence can play a significant role in affecting the risk calculations of malicious actors. However, in the digital world, those who combat cybercrime have yet to develop or implement this type of enforcement model. When private actors report cyber incidents, they may or may not be investigated depending on enforcement priorities. Where investigations do take place, they often are completed in a less visible manner, or worse, lead to penalties on the victims.

32. See for example John P. Carlin, "Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats," *Harvard National Security Journal Vol. 7* (2016), http://harvardnsj.org/wp-content/uploads/2016/06/Carlin-FINAL.pdf.

33. The United States Department of Defense defines passive defense as "measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative." *Joint Publication (JP) 1-02 Dictionary of Military and Associated Terms.* U.S. Department of Defense, March 2015. Robert M. Lee, "The Sliding Scale of Cyber Security," *SANS Analyst White Paper, SANS Institute InfoSec Reading Room* (2015), https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240.

34. Lee, "The Sliding Scale of Cyber Security," 7.

35. Ibid.

36. General William E. DePuy, "Implications of the Middle East War on U.S. Army Tactics, Doctrine and Systems," *The William E. DePuy Papers, Command History Office, U.S. Army Training and Doctrine Command* (1974), http://usacac.army.mil/cac2/cgsc/carl/download/csipubs/SelectedPapersofGeneralWilliamDepuy.pdf quoted in Lee, "The Sliding Scale of Cyber Security," 9.

37. General William E. DePuy, *FM 100-5 Revisited, (1980),* quoted in Lee, "The Sliding Scale of Cyber Security," 9.

38. Lee, "The Sliding Scale of Cyber Security," 10.

39. Ibid.

40. U.S. Department of Defense, *Joint Publication (JP) 1-02 Dictionary of Military and Associated Terms,* (2012) quoted in Lee, "The Sliding Scale of Cyber Security," 10.

41. The Department of Defense's Advanced Research Projects Agency first operated the predecessor to the Internet, known as ARPANET, based on packet switching technology developed in 1969. "Cyber" probably first began entering military lexicon in the 1980s and the early instances of cyber doctrine in warfare may have occurred in the mid-1990s during Operation Desert Storm. Edward M. Roche, *Dark Territory: The Secret History of Cyber War*, 2 *Journal of Strategic Security* 9 (2016), 122.

42. Lee, "The Sliding Scale of Cyber Security," 8.

43. Ibid.

44. Lee, "The Sliding Scale of Cyber Security," 10.

45. Ibid.

46. Timothy B. Lee, "How a grad student trying to build the first botnet brought the Internet to its knees," *Washington Post,* November 1, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees.

47. Ruperto P. Majuca & Jay P. Kesan, "Hacking Back: Optimal Use of Self-Defense in Cyberspace," Illinois P.L. & Legal Theory Paper Series No.08-20, March 18, 2009, papers.ssrn.com/sol3/papers.cfn?abstract id=1363932.

48. "Press Release, Symbiot Security Announces World's First Solution to Strike Back Against Network-Based Attackers." *Symbiot, Inc.* (2004), https://web.archive.org/web/20080908021351/http://www.symbiot.com/pdf/pr.030404.pdf quoted in Majuca et al. "Hacking Back: Optimal Use of Self-Defense in Cyberspace," 5.

49. Paco X. Nathan et al. "On the Rules of Engagement for Information Warfare" Symbiot, Inc. (2004), https://web.archive.org/web/20120206030024/http://www.symbiot.com/pdf/iwROE.pdf quoted in Majuca et al. "Hacking Back: Optimal Use of Self-Defense in Cyberspace," 5.

50. Ibid, 4.
51. Sarah Sorcher, "Influencers: Companies should not be allowed to hack back," *Passcode, The Christian Science Monitor,* April 1, 2016, http://www.csmonitor.com/World/Passcode/Passcode-Influencers/2015/0401/Influencers-Companies-should-not-be-allowed-to-hack-back.
52. Ibid.
53. See Kim Zetter, *Countdown to Zero Day*, 2014, for a discussion of Stuxnet.
54. It is important to note that while hacking back is offensive in nature, military and intelligence officers tend to place it in a category of action that is distinct from the sophisticated and tailored approaches that they consider "cyber offense." While the intelligence collection potentials of hacking back may appear attractive to private companies, there are other less risky methods to gather such information that should always be prioritized.
55. Robert Belk & Matthew Noyes, "On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy," Paper, *Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs*, Harvard Kennedy School (March 2015).
56. Ibid.
57. Impact is measuring the effectiveness of such techniques at deterring cyber threats, and risk is the level of exposure a defender assumes to potential adverse effects such as escalation, unintended consequences, misattribution, and civil or criminal liability.
58. Kristen Heckman et al., "Cyber Denial, Deception, and Counter Deception: A Framework for Supporting Active Cyber Defense," *Springer International Publishing* (2015), http://www.springer.com/us/book/9783319251318.
59. Dye packs are an inherently riskier measure than beacons from a legal standpoint, given that they install malware on an attacker's system after data exfiltration.
60. European Union Agency for Network and Information Security, "DNS Sinkhole" (accessed Oct. 14, 2016), https://www.enisa.europa.eu/topics/national-csirt-network/glossary/dns-sinkhole.
61. Kim Zetter, "'Google' Hackers Had Ability to Alter Source Code," *Wired,* March 3, 2010, https://www.wired.com/2010/03/source-code-hacks.
62. David E. Sanger & John Markoff, "After Google's Stand on China, U.S. Treads Lightly," *New York Times-* January 15, 2010, http://www.nytimes.com/2010/01/15/world/asia/15diplo.html?ref=technology&_r=0.
63. Shane Harris, "Google's Secret NSA Alliance: The terrifying deals between Silicon Valley and the Security State," *Salon-* November 16, 2014, http://www.salon.com/2014/11/16/googles_secret_nsa_alliance_the_terrifying_deals_between_silicon_valley_and_the_security_state.
64. Shane Huang, "Proposing a Self-Help Privilege for Victims of Cyber Attacks," *82 Geo. Wash. L. Rev. 1228- 1249–50.*
65. "Best Practices for Victim Response and Reporting of Cyber Incidents," *Cybersecurity Unit, Computer Crime & Intellectual Property Section, U.S. Department of Justice*, April 29, 2015, https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf.
66. DOJ Press Release - Partners involved in the Dridex/Bugat takedown include the FBI, DHS' US-CERT, the UK National Crime Agency, Europol's EC3, Germany's Bundeskriminalamt, Dell SecureWorks, Trend Micro, Fox-IT, S21sec, Abuse.ch, the Shadowserver Foundation, Spamhaus, and the Moldovan General Inspectorate of Police Centre for Combatting Cybercrime, the Prosecutor General Office Cyber Crimes Unit, and the Ministry of Interior Forensics Unit.
67. Jai Vijayan, "Dridex Malware Now Used for Stealing Payment Card Data," *Dark Reading*, April 8, 2016, http://www.darkreading.com/vulnerabilities---threats/dridex-malware-now-used-for-stealing-payment-card-data/d/d-id/1325056.
68. John Leyden, "FBI Takes Down Dridex Botnet, Seizes Servers, Arrests Suspects," *The Register*, October 14, 2015, http://www.theregister.co.uk/2015/10/14/dridex_botnet_takedown.
69. Ericka Chickowski, "Dridex Takedown Might Show Evidence of Good Guys' Gains," *Dark Reading*, October 14, 2015, http://www.darkreading.com/attacks-breaches/dridex-takedown-might-show-evidence-of-good-guys-gains/d/d-id/1322658.
70. "Bugat Botnet Administrator Arrested and Malware Disabled," U.S. Department of Justice, Office of Public Affairs, October 13, 2015, https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/bugat-botnet-administrator-

arrested-and-malware-disabled.

71. "UK Internet Users Potential Victims of Serious Cyber Attack," *UK National Crime Agency,* October 13, 2015, http://www.nationalcrimeagency.gov.uk/news/723-uk-internet-users-potential-victims-of-serious-cyber-attack.

72. Hadi Asghari, Michael Ciere, and Michael van Eeten, "Post Mortem of a Zombie: Conficker Cleanup after Six Years," *Usinex Security Symposium,* August 2015, https://www.usenix.org/node/190883.

73. Michael van Eeten et al., "The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis based on Spam Data," *Organisation for Economic Cooperation and Development*, November 12, 2010 http://www.oecd-ilibrary.org/science-and-technology/the-role-of-internet-service-providers-in-botnet-mitigation_5km4k7m9n3vj-en.

74. Department of Justice Office of Public Affairs, "Bugat Botnet Administrator Arrested And Malware Disabled," October 13, 2015, https://www.justice.gov/opa/pr/bugat-botnet-administrator-arrested-and-malware-disabled.

75. Torsten Ove, "Moldovan Hacker Smilex Charged in Court after being Extradited from Cyprus," *Pittsburgh Post-Gazette*, February 26, 2016, http://www.post-gazette.com/local/city/2016/02/26/Moldovan-hacker-Smilex-charged-in-email-phishing-scheme-appears-in-court/stories/201602260259.

76. Brian Donohue, "What is APT?," *KaperskyLab Daily*, June 11, 2013, https://blog.kaspersky.com/apt/2050 (detailing the unusual sophistication, precision, and persistence of APTs).

77. Office of the National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011," October 2011, https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf.

78. *See infra* Appendix II: Legal Analysis at 44.

79. Eugene Volokh, Stewart Baker, and Orin Kerr, "The Hackback Debate," *Steptoe Cyber Blog*- November 2, 2012, http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate. Debating the legality of hacking back under the CFAA, the federal common law defenses of Defense of Property and Necessity, and the Model Penal Code §3.06; Mark Rasch, "Legal Issues in Penetration Testing," *Securitycurrent*- November 26, 2013, http://www.securitycurrent.com/en/analysis/ac_analysis/legal-issues-in-penetration-testing, discussing the issue of implied consent in penetration testing and active defense activities.

80. Ibid.

81. Bret Jordan, "STIX and TAXII: On the road to becoming the de facto standard," *Blue Coat Systems Inc.,* August 26, 2014, https://www.bluecoat.com/security-blog/2014-08-26/stix-and-taxii-road-becoming-de-facto-standard.

82. Shubhomita Bose, "85 Percent of Small Businesses Set to Invest More in SaaS," *Small Business Trends,* July 28, 2016, http://smallbiztrends.com/2016/07/saas-industry-trends-small-business.html; *2016 Report on the State of SaaS*, https://www.betterbuys.com/the-state-of-saas.

83. Chris Bing, "Small business cybersecurity lagging as attacks increase—security experts," *FedScoop,* July 7, 2016, http://fedscoop.com/small-business-cybersecurity-lacking-while-attacks-increase-say-security-experts.

84. Michael J. Covington and Rush Carskadden, "Threat Implications of the Internet of Things," in K. Podins, J. Stinissen, and M. Maybaum (Eds.), *2013 5th International Conference on Cyber Conflict,* 2013 NATO CCD COE Publications, Tallinn, https://ccdcoe.org/cycon/2013/proceedings/d1r1s6_covington.pdf.

85. Hannah Kuchler, "Cyber insecurity: Hacking Back," *Financial Times,* July 27, 2015, https://www.ft.com/content/c75a0196-2ed6-11e5-8873-775ba7c2ea3d.

86. Shaun Donovan, Beth Cobert, Michael Daniel, and Tony Scott, *Strengthening the Federal Cybersecurity Workforce,* July 12, 2016, https://www.whitehouse.gov/blog/2016/07/12/strengthening-federal-cybersecurity-workforce.

87. Article 2—Illegal Access. Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally, the access to the whole or any part of a computer system **without right. A Party may require that the offence be committed by infringing security measures with the intent of obtaining computer data or other dishonest intent,** or in relation to a computer system that is connected to another computer system. Convention on Cybercrime, Council of Europe, November 23, 2011, T.S. No. 185, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185.

88. *See infra* Appendix II: Legal Analysis at 44.

89. Paul Ferrillo, "Grading Global Boards of Directors on Cybersecurity," *Harvard Law School Forum on Corporate Governance and Financial Regulation,* May 1, 2016, https://corpgov.law.harvard.edu/2016/05/01/grading-global-boards-of-directors-on-cybersecurity.

90. "Barracuda, Reversinglabs, Telefonica and Zscaler Join Cyber Threat Alliance as Contributing Members," *PaloAltoNetworks.com*, Feb. 13, 2015, http://investors.paloaltonetworks.com/phoenix.zhtml?c=251350&p=irol-newsArticle_Print&ID=2016614.

91. "Lucrative Ransomware Attacks: Analysis of the CryptoWall Version 3 Threat," *Cyber Threat Alliance* (2015), http://www.cyberthreatalliance.org/cryptowall-executive-summary.pdf.

92. For a discussion on the distinction between defense and deterrence-by-denial, *see* Franklin Kramer & Melanie Teplinsky, "Cybersecurity and Tailored Deterrence," *Atlantic Council Issue Brief* (2013), http://www.atlanticcouncil.org/images/publications/Cybersecurity_and_Tailored_Deterrence.pdf.

93. Michael Riley & Jordan Roberson, "FBI Probes If Banks Hacked Back as Firms Mull Offensives," *Bloomberg*, December 30, 2014, http://www.bloomberg.com/news/articles/2014-12-30/fbi-probes-if-banks-hacked-back-as-firms-mull-offensives.

94. Ibid.

95. DJ Summers, "As cyber attacks swell, a move toward improved industry collaboration," *Fortune*, January 7, 2015, http://fortune.com/2015/01/07/cybersecurity-collaboration.

96. Tova Cohen, "U.S. and Israeli Startups Lead the Way in New Cyber Security Tricks," *Haaretz*, January 27, 2016, http://www.haaretz.com/israel-news/business/1.699916.

97. Alan Charles Raul, "Cyberdefense Is a Government Responsibility," *Wall Street Journal*, January 5, 2015, http://www.wsj.com/articles/alan-charles-raul-cyberdefense-is-a-government-responsibility-1420502942.

98. Larry Karisnky, "Cybersecurity: A Millisecond Defense," *GovTech: Digital Communities,* November 12, 2015, http://www.govtech.com/dc/articles/Cybersecurity-A-Millisecond-Defense.html.

99. Lisa Monaco, "Expanding Our Ability to Combat Cyber Threats," *The White House (Blog)*, April 1, 2015, https://www.whitehouse.gov/blog/2015/04/01/expanding-our-ability-combat-cyber-threats. See also Presidential Policy Directive-41, 2016, and the related Cyber Incident Severity Schema, available at https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/Cyber+Incident+Severity+Schema.pdf

100. Eyragon Eidam, "Report: What is the U.S. Government's Role in Cybersecurity?," *GovTech,* August 31, 2015, http://www.govtech.com/federal/Report-What-is-the-US-Governments-Role-in-Cybersecurity.html.

101. Dan Klinedinst, "Coordinating Vulnerabilities in IoT Devices," *CERT/CC (Blog), Software Engineering Institute Carnegie Mellon University,* January 27, 2016, https://insights.sei.cmu.edu/cert/2016/01/coordinating-vulnerabilities-in-iot-devices.html.

102. *Computer Fraud and Abuse Act, U.S. Code 18* (2012), §1030(f).

103. Leslie R. Caldwell, "Assistant Attorney General Leslie R. Caldwell Delivers Remarks at the Georgetown Cybersecurity Law Institute," *Cybersecurity Law Institute*, May 20, 2015, https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-georgetown-cybersecurity.

104. Ibid.

105. Josh Johnson "Implementing Active Defense Systems on Private Networks," *InfoSec Reading Rom SANS Institute* (2013), https://www.sans.org/reading-room/whitepapers/detection/implementing-active-defense-systems-private-networks-34312 (discussing the implementation of active defense measures along the lines of the "cyber kill chain").

106. Irving Lachow, "Active Cyber Defense, A Framework for Policymakers," Policy Brief, *Center for a New American Security* (2013), https://s3.amazonaws.com/files.cnas.org/documents/CNAS_ActiveCyberDefense_Lachow_0.pdf.

107. Ibid.

108. Paul Rosenzweig, *International Law and Private Actor Active Cyber Defensive Measures,* Stanford J. Int'l L. 47 (2013).

109. Ibid, 4. ("…[such] a typology then helps us **identify the appropriate legal régimes** that would apply in various domains. We can ask a sensible question like 'what should be the legal limits of a private sector actors [sic] off-network attribution efforts that have no appreciable effect?' and mean something that actually says 'is this beaconing technique legal?'") (emphasis original).

110. Anthony D. Glosson, "Active Defense: An Overview of the Debate and a Way Forward" *Mercatus Working Paper* (2015), http://mercatus.org/sites/default/files/Glosson-Active-Defense.pdf (citing Google's Operation Aurora, Facebook's campaign against "Koobface," and Conxion's reversal of a DOS attack on the World Trade Organization against a collection of "electrohippies").

111. Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information, Department of Justice & Federal Trade Commission (2014), https://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf.

112. Companies conducting "lawfully authorized investigative, protective, or intelligence activit[ies]" are excluded from the CFAA's criminal provisions under *Computer Fraud and Abuse Act, U.S. Code 18* (2012), §1030(f).

113. Jeffery Meisner, "Microsoft Works with Financial Services Industry Leaders, Law Enforcement and Others to Disrupt Massive Financial Cybercrime Ring," *The Official Microsoft Blog*, June 5, 2013, https://blogs.technet.microsoft.com/microsoft_blog/2013/06/05/microsoft-works-with-financial-services-industry-leaders-law-enforcement-and-others-to-disrupt-massive-financial-cybercrime-ring (others involved included the Financial Services-Information Sharing and Analysis Center, the American Bankers Association, and foreign Computer Emergency Response Teams). Though the Citadel takedown made a substantial impact on the botnet's operation, it is extremely difficult to totally eliminate a botnet since it can so easily be reconstructed and redirected. Law enforcement continues to work to prosecute the operators of the botnets in order to address the problem at its source instead of just treating the symptoms. See ibid.

114. Microsoft has been accused of using *ex parte* preliminary restraining orders overzealously to seize domain names hosting both legitimate and illegitimate traffic, harming innocent third parties. Robert McMillan, "How Microsoft Appointed Itself the Sheriff of the Internet," *Wired*, October 16, 2014, http://www.wired.com/2014/10/microsoft-pinkerton.

115. Jeremy Rabkin & Ariel Rabkin, "Hacking Back Without Cracking Up," *Hoover Institution*, Series Paper No. 1606 (2016), http://www.hoover.org/sites/default/files/research/docs/rabkin_finalfile_2.pdf#overlay-context=.

116. Ibid, 14.

117. William Roth, "Cyber Attacks Against the U.S.: Deputizing the Private Sector to Assist," (2016). Drawing an analogy between licensed cybersecurity firms authorized to engage in limited intelligence gathering techniques on external networks and U.S. State licensure of railroad police of limited powers "in situations where government is incapable" of keeping the peace.

118. Rabkin, "Hacking Back," 4–5.

119. Ibid, 10.

120. Ibid, 11.

121. For an overview of various legal regimes applicable to Active Defense techniques, see Appendix II: Legal Analysis at 44.

122. U.N. General Assembly. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." *UN document A/65/201* 30 (2010), http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

123. Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press (2013), https://ccdcoe.org/tallinn-manual.html.

124. Convention on Cybercrime, Council of Europe, November 23, 2011, T.S. No. 185, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185.

125. Paul Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures," *Stanford J. Int'l L. 47* (2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2270673.

126. Christopher Painter, "G20: Growing International Consensus on Stability in Cyberspace," *DIPNOTE*, December 3, 2015, http://blogs.state.gov/stories/2015/12/03/g20-growing-international-consensus-stability-cyberspace.

127. Ariel Rabkin & Jeremy A. Rabkin, "Enhancing Network Security: A Cyber Strategy for the Next Administration," *American Enterprise Institute*, May 2016, 14-17, https://www.aei.org/wp-content/uploads/2016/05/Enhancing-network-security.pdf.

128. Exec. Order No. 13,636, 3 C.F.R. § 13636 (2013), https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf.

129. "Distributed environments face a variety of unique challenges that make security administrators' tasks even harder. Not only do they often have access rules that vary by business unit, but their traditional firewall rules are frequently complex and

unmanageable as well. In addition, distributed environments usually have federated, if not chaotic, endpoint governance. Data is further exposed because more copies of data create more places where it needs to be protected." John Pescatore, "Conquering Network Security Challenges in Distributed Enterprises," *SANS Institute, InfoSec Reading Room*, June 2015, https://www.sans.org/reading-room/whitepapers/analyst/conquering-network-security-challenges-distributed-enterprises-36007.

130. The Department of Homeland Security and The Department of Justice, "Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015," (June 15, 2016), available at: https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_(Sec%20105(a)).pdf.

131. Nate Cardozo, "What Were They Thinking? Microsoft Seizes, Returns Majority of No-IP.com's Business,"*Deep Links*, The Electronic Frontier Foundation (July 10, 2014), available at: https://www.eff.org/deeplinks/2014/07/microsoft-and-noip-what-were-they-thinking.

132. Jadzia Butler, "U.S. Supreme Court Endorses Government Hacking" The Center for Democracy & Technology, (May 6, 2016), available at: https://cdt.org/blog/u-s-supreme-court-endorses-government-hacking.

133. HM Government. 2010. *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf; details on the Cyber-security Information Sharing Partnership (CiSP) are available at https://www.cert.gov.uk/cisp.

134. Martin Arnold, "Hacking Onslaught Tests UK Banks' Defences," *Financial Times*, May 18, 2015, http://www.ft.com/cms/s/0/3789c838-fd5f-11e4-9e96-00144feabdc0.html#axzz4GUXKRzmL.

135. UK Cabinet Office, "New National Cyber Security Centre Set to Bring UK Expertise Together," Press Release: March 18, 2016, https://www.gov.uk/government/news/new-national-cyber-security-centre-set-to-bring-uk-expertise-together.

136. Harry Wilson, "Millions Affected after Cyber Attack on HSBC," *The Telegraph*, October 19, 2012, http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/9621883/Millions-affected-after-cyber-attack-on-HSBC.html; Olivia Rudgard, "HSBC Online Banking Failure: What You Need to Know," *The Telegraph*, January 29, 2016, http://www.telegraph.co.uk/finance/personalfinance/bank-accounts/12129786/HSBC-online-banking-fails-again-after-succumbing-to-cyber-attack.html.

137. Ryan Huang, "StanChart Client Data Stolen in Singapore via Fuji Xerox server," *ZDNet*, December 6, 2013, http://www.zdnet.com/article/stanchart-client-data-stolen-in-singapore-via-fuji-xerox-server.

138. Hayley Dixon, "Barclays Hacking Attack Gang Stole £1.3 million," *The Telegraph*, September 20, 2013, http://www.telegraph.co.uk/news/uknews/crime/10322536/Barclays-hacking-attack-gang-stole-1.3-million-police-say.html.

139. Martin Arnold, Tom Brathwaite, and Hannah Kuchler, "Davos 2015: Banks Call for Free Rein to Fight Cyber Crime," *Financial Times*, January 22, 2015, https://next.ft.com/content/d94e855c-a209-11e4-bbb8-00144feab7de.

140. Ibid.

141. Hannah Kuchler, "Cyber insecurity: Hacking back," *Financial Times*, July 27, 2015, https://next.ft.com/content/c75a0196-2ed6-11e5-8873-775ba7c2ea3d.

142. Jack Goldsmith, "On French Espionage," *Lawfare*, July 5, 2013, https://www.lawfareblog.com/french-espionage.

143. Anne-Sylvaine Chassany & Michael Stothard, "France beefs up defences against corporate espionage," *Financial Times*, May 8, 2016, https://www.ft.com/content/2ee985c2-14f8-11e6-b197-a4af20d5575e.

144. Danilo D'Elia, "Military Programming Laws and Protecting Essential Services Operators," *Chaire Castex de Cyberstratégie*, February 13, 2014, http://www.cyberstrategie.org/?q=en/military-programming-laws-and-protecting-essential-services-operators.

145. Aline Doussin, "New EU Cybersecurity Requirements Soon to Fall on 'Essential Services' Operators," *Global IP & Privacy Law Blog*, May 29, 2016, http://www.iptechblog.com/2016/05/new-eu-cybersecurity-requirements-soon-to-fall-on-essential-services-operators.

146. Hugh Schofield, "Surveillance Law Prompts Unease in France," *BBC News*, May 4, 2015, http://www.bbc.com/news/world-europe-32497034.

147. "Un service à compétence nationale rattaché à la direction générale des entreprises," *Ministère de l'Économie, de l'Industrie et du Numérique*, February 3, 2016, http://www.economie.gouv.fr/institution-d-un-commissaire-a-l-information-strategique-et-a-la-securite-economiques.

148. Daniel Severson, "Encryption Legislation Advances in France," *Lawfare*, April 14, 2016, https://www.lawfareblog.com/encryption-legislation-advances-france.

149. Jean-Baptiste Vey & Geert De Clercq, "France says Fight Against Messaging Encryption needs Worldwide Initiative," *Reuters,* August 11, 2016, http://www.reuters.com/article/us-france-internet-encryption-idUSKCN10M1KB.

150. The Center for Cyber and Homeland Security would like to thank Patrik Maldre and Sander Retel of Retel Partners for sharing their insights into the active defense climate of Estonia.

151. Anna-Maria Osula. "National Cyber Security Organization: Estonia." *NATO Cooperative Cyber Defence Centre of Excellence* (2015), https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_ESTONIA_032015_1.pdf.

152. Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, May 16, 2007, https://www.theguardian.com/world/2007/may/17/topstories3.russia.

153. Ministry of Economic Affairs and Communications. 2014. Estonia—*Cyber Security Strategy 2014-2017* (2014), https://www.mkm.ee/en/objectives-activities/information-society/cyber-security.

154. "Estonia Supports Council of Europe's Fight Against Cybercrime" *Estonian Ministry of Foreign Affairs*: Press Release, September 13, 2013, http://vm.ee/en/news/estonia-supports-council-europes-fight-against-cybercrime-1.

155. "Estonian Cybercriminal Sentenced For Infecting 4 Million Computers In 100 Countries With Malware In Multimillion-Dollar Fraud Scheme." *Department of Justice, U.S. Attorney's Office Southern District of New York:* Press Release, April 26, 2016, https://www.justice.gov/usao-sdny/pr/estonian-cybercriminal-sentenced-infecting-4-million-computers-100-countries-malware.

156. James Lewis, "Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States," *Inter-American Development Bank* (2016), https://publications.iadb.org/bitstream/handle/11319/7759/Advanced-Experiences-in-Cybersecurity-Policies-and-Practices-An-Overview-of-Estonia-Israel-South-Korea-and-the-United%20States.pdf?sequence=2.

157. John Reed, "Israel Cyber-security Expertise Lures Growing Share of Investment," *Financial Times*, January 12, 2016, https://www.ft.com/content/dfa5c916-b90e-11e5-b151-8e15c9a029fb.

158. Michael Raska, "Building a Cyber Iron Dome: Israel's Cyber Defensive Envelope," *S. Rajaratnam School of International Studies* (2014), https://www.rsis.edu.sg/rsis-publication/rsis/co14192-building-a-cyber-iron-dome-israels-cyber-defensive-envelope/#.V-Wq1SErLcs.

159. Ibid.

160. Lewis, "Advanced Experiences."

161. Neal Ungerleider, "How Eric Schmidt, Cisco, and an Israeli Spymaster Launched a New Cybersecurity Incubator," *Fast Company* (2015), https://www.fastcompany.com/3042158/googles-eric-schmidt-cisco-israeli-spymaster-behind-new-cybersecurity-incubator-team8-ventur.

162. Matthew Cohen, Charles Freilich, and Gabi Siboni, "Israel and Cyberspace: Unique Threat and Response," *International Studies Perspectives,* December 29, 2015, http://belfercenter.hks.harvard.edu/publication/26135/israel_and_cyberspace.html?breadcrumb=%2Findex; Embassy of Israel in India, "Digital Israel—National Initiative," March 2, 2014, http://embassies.gov.il/delhi/NewsAndEvents/Pages/Digital%20Israel%20%E2%80%93%20National%20Initiative.aspx; Orr Hirshauge, Inbal Orpaz, and Amitai Ziv, "Is the Israeli Government Taking its High-tech Aspirations too Far?" December 11, 2013, http://www.haaretz.com/.premium-1.562795.

163. Lewis, "Advanced Experiences."

Selected Works Consulted

Baker, Stewart, and Orin Kerr, Eugene Volokh. "The Hackback Debate." *Steptoe Cyber Blog.* 2012.

Blair, Dennis and Jon M. Huntsman, Jr., "The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property." *The National Bureau of Asian Research*. May 2013.

Center for Strategic and International Studies and U.S. Department of Justice, "Summary of Active Defense Cyber Experts Roundtable." March 10, 2015.

Chabinsky, Steven. "A Primer for Policymakers and those on the Front Line." *4 J. Nat'l Security L. & Pol'y 27.* 2010.

Computer Crimes Intellectual Property Section Criminal Division. Office of Legal Education, Executive Office for United States Attorneys. "Prosecuting Computer Crimes." January 14, 2015.

Conti, Gregory et al. "The Ethics of Hacking Back: Cybersecurity and Active Network Defense." *Carnegie Council for Ethics in International Affairs.* October 25, 2013.

Council on Cybersecurity. "The Critical Security Controls for Effective Cyber Defense." *Critical Security Controls Version 5.0.* February 2, 2014.

Denning, Dorothy. "Framework and Principles for Active Cyber Defense." *Computers & Security 40. Elsevier.* 108-113. February 2014.

Denning, Dorothy. "Rethinking the Cyber Domain and Deterrence." *Joint Force Quarterly 77.* 2nd Quarter. 2015.

Fick, Nathaniel. "Learning to Win: Lessons from One Domain of Conflict for Another." Infiltrate Security Conference. Speech. April 7, 2016.

Goodman, Seymour & Herbert Lin. "Toward a Safer and More Secure Cyberspace." *National Research Council and National Academy of Engineering of the National Academies. The National Academies Press.* 2007.

Harrington, Sean L. "Cyber Security Active Defense: Playing with Fire or Sound Risk Management?" *20 Richmond Journal of Law & Technology. 12* (2014).

Healey, Jason. "White Paper on Information Warfare Terms." March 1999.

Heckman, Kristin E. et al. "Cyber Denial Deception and Counter Deception: A Framework for Supporting Active Defense." *Advances in Information Security Volume 63. Springer International Publishing.* Switzerland. 2015.

Huang, Shane. "Proposing a Self-Help Privilege for Victims of Cyber Attacks." *82 Geo. Wash. L. Rev. 1229.* August 2014.

Johnson, John. "Implementing Active Defense Systems on Private Networks." *SANS Institute Reading Room. SANS Institute.* 2013.

Kerr, Orin S. "Norms of Computer Trespass." *116 Columbia Law Review 1143* (2016); *GWU Law School Public Research Paper No. 2015-17*; *GWU Legal Studies Research Paper No. 2015-17.* (May 2, 2015).

Kesan, Jay & Carol Hayes. "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace." *Harvard Journal of Law & Technology Vol. 25 No. 2.* 2012.

Kesan, Jay & Carol Hayes. "Self Defense in Cyberspace: Law and Policy." *Illinois Program in Law. Behavior and Social Science Research Paper No. LBSS12-08. Illinois Public Law and Legal Theory Research Paper Series No. 11-16.* 24 September 2011.

Lachow, Irving. "Active Cyber Defense: A Framework for Policy Makers." *Center for a New American Security.* February 2013.

Lerner, Zach. "Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets." *Harvard Journal of Law & Technology Vol. 28 No. 1.* Fall 2014.

Li, Sheng. "When does Internet Denial Trigger the Right of Armed Self Defense?" *38 Yale J. Int'l L. 179.* 2013.

Lin, Herbert. "Offensive Cyber Operations & the Use of Force." *4 J. Nat'l Security L. & Pol'y 63.* 2010.

Lin, Patrick. "Ethics of Hacking Back: Six Arguments from Armed Conflict to Zombies." Ethics and Emerging Sciences Group, California Polytechnic State University, San Luis Obispo. September 26, 2016.

McGee, Sharon, et al. "Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense." *8 J. Bus. & Tech. L. 1.* 2012.

Martemucci, Matteo. "Unpunished Insults: The Looming Cyber Barbary Wars." *Case Western Reserve Journal of International Law 47.* 2015.

Messerschmidt, Jan. "Hackback: Permitting Retaliatory Hacking by Non-state Actors as Proportionate Countermeasures to Cyberharm." *52 Colum. J. Transnat'l L. 275.* 2013.

Rosenzweig, Paul, International Law and Private Actor Active Cyber Defensive Measures." *Stanford Journal of International Law, Vol. 47.* May 27, 2013.

Rosenzweig, Paul. "Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Opinions for US Policy." *National Research Council of the National Academies. National Academies Press.* 2010.

Rowe, Elizabeth A., "RATs, TRAPs, and Trade Secrets." *Boston College Law Review.* September 17, 2015.

Schmitt, Michael. "International Law in Cyberspace: The Koh Speech and

Tallinn Manual Juxtaposed." *Harvard International Law Journal Online Vol. 54.* December 2012.

U.S. Congress. Senate. Committee on the Judiciary. *Hearing - Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks.* 113th Cong., 2nd sess., July 15, 2014 (Statement of Cheri McGuire, Vice President, Global Government Affairs & Cybersecurity Policy, Symantec Corporation).

U.S. Congress. House. Committee on Science, Space and Technology. *Hearing - The Expanding Cyber Threat.* 114th Cong. 1st sess., January 27, 2015 (Statement of Cheri McGuire, Vice President, Global Government Affairs & Cybersecurity Policy, Symantec Corporation).

West, Zach. "Deputizing Private Companies for the use of Hackback." *63 Syracuse L. Rev. 119.* 2012.

Wong, Tiong. "Active Cyber Defense: Enhancing National Cyber Defense." Calhoun: The NPS Institutional Archive. *Naval Postgraduate School.* December 2011.

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 non-partisan "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.

Into the Gray Zone...

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.

Center for Cyber
& Homeland Security

THE GEORGE WASHINGTON UNIVERSITY

2000 Pennsylvania Avenue · Washington D.C., 20052
cchs.gwu.edu