
PRIVATE
SECTOR
CYBER
DEFENSE
Can Active Measures
Help Stabilize Cyberspace?
WYATT HOFFMAN AND ARIEL E. LEVITE

PRIVATE SECTOR CYBER DEFENSE

Can Active Measures Help Stabilize Cyberspace?

WYATT HOFFMAN AND ARIEL E. LEVITE

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue, NW
Washington, DC 20036
P: +1 202 483 7600
F: +1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org/pubs.

TABLE OF CONTENTS

ABOUT THE AUTHORS

WYATT HOFFMAN is a nonresident research analyst with the Nuclear Policy Program and the Cyber Policy Initiative at the Carnegie Endowment for International Peace. He is also a Rotary Global Grant scholar in the Department of War Studies at King's College London. His research focuses on active cyber defense in the private sector, norms for cyberwarfare, and the intersection of nuclear weapons and cybersecurity. He previously worked as a project manager and junior fellow with the Nuclear Policy Program at Carnegie.

ARIEL E. LEVITE is a nonresident senior fellow with the Nuclear Policy Program and the Cyber Policy Initiative at the Carnegie Endowment for International Peace. Prior to joining Carnegie in 2008, Levite was the principal deputy director general for policy at the Israeli Atomic Energy Commission from 2002 to 2007. He earlier served as the deputy national security adviser for defense policy and was head of the Bureau of International Security and Arms Control (an assistant secretary position) in the Israeli Ministry of Defense.

ACKNOWLEDGMENTS

This report benefited immeasurably from extensive consultations worldwide with numerous individuals in the private sector (ICT industry, insurance, and finance), government, thinks tanks, and academia. Gathered over the course of a year, their input directly informed both the research and writing processes. In particular, we would like to thank George Perkovich, Scott Kannry, Tim Maurer, Joel Brenner, Steven Weber, Brendan Fitzpatrick, Irving Lachow, and Gare Smith for their invaluable feedback, ideas, and contributions. George Perkovich also deserves much credit for his unflinching support and encouragement and for painstakingly commenting on and editing several drafts of this report. We would also like to thank Steven Nyikos for his considerable support.

SUMMARY

The cyber revolution and ever-growing transfer of human activities into the virtual world are undermining the social contract between modern states and their citizens. Most governments are becoming unable and unwilling to protect citizens and private enterprises against numerous, sophisticated cyber predators seeking to disrupt, manipulate, or destroy their digital equities. Inevitably, states are focused on protecting governmental assets and national infrastructure, leaving themselves with modest residual capacity and resolve to underwrite other cybersecurity risks. Faced with this reality, private entities are reluctantly but increasingly complementing their passive cybersecurity practices with more assertive "active cyber defense" (ACD) measures. This approach carries substantial risks, but if guided by bounding principles and industry models, it also has the potential for long-term, cumulative benefits.

REGULATING AN EMERGING INTERNATIONAL MARKET

The limitations of governance. States are struggling to find a viable formula to regulate emerging private sector cyber activity. The challenge is compounded by the global and rapidly evolving nature of the cyber domain. Consequently, in many countries, national laws governing this space are either absent, vague, or difficult to operationalize. International understanding and conventions to harmonize national responses are also largely absent, complicating efforts to manage cross-border incidents with political ramifications.

The benefit of experience. The shipping industry's experience with resurging piracy offers valuable insights. After it became clear that governments' military efforts were insufficient responses to the problem, the demand for private sector security services increased dramatically. While governments initially resisted their involvement, they begrudgingly accepted that the active defense measures deployed by shipowners, in consultation with insurance providers, were helping to deter attacks and that the tradeoffs in risk were unavoidable. The bottom line—the private sector filled a critical gap in protection.

INCENTIVIZING BEHAVIOR FOR MINIMUM RISK, MAXIMUM BENEFIT

A principles-based approach. To fill the vacuum in the cyber domain, companies are engaging attackers within and outside of the defender's network to preempt, interfere with, or mitigate the consequences of cyberattacks. Rather than trying to enforce ineffectual laws and regulations, governments and stakeholders should seek to develop guiding principles for a spectrum of ACD, excluding "hacking back." Such principles could be embedded in a range of mechanisms, for example a voluntary code of conduct for employing ACD.

An industry-driven model. International and domestic market mechanisms, including a corporate social responsibility initiative, could provide the incentives to ensure voluntary adherence to the principles and code and a degree of accountability. The insurance industry in particular could play a large role in minimizing risk and generating economic advantages for not just defenders but also those working with them or receiving their services.

INTRODUCTION

The cybersecurity domain has reached a critical juncture. Human and commercial reliance on Information and Communications Technology (ICT) has become absolutely germane in both commercial and private life. This dependence keeps on growing by the day. But with it has come rapid growth in criminal, terrorist, ideological, and security driven attacks on the ICT infrastructure and the functions it serves. At least for now, attackers seem to have the upper hand. And the prospects for the near term hardly look better.

Cybersecurity threats are multiplying. Costs and liabilities associated with cyberattacks are escalating. And while some governments are proving successful in deterring attacks and protecting governmental assets and critical national infrastructure, almost all are proving unwilling and/or unable to extend cybersecurity to the private sector. Most governments eschew a formal commitment to defend the private sector against cyberattacks, manifesting serious shortcomings in pursuing cyber offenders while also exercising deliberative restraint in responding to external threats and attacks directed at private entities based on their soil. Further compounding the cyber threat challenge facing private sector entities is the serious difficulty of obtaining adequate insurance to cover for substantial risks or potential losses (beyond physical damages) incurred. Evolving tactics by malicious actors to cripple the services of private entities (a la Dyn),[1] steal their intellectual property (as was the case with the 2014 Sony hack), or hold their critical data hostage (such as the most recent widespread use of ransomware) only illustrate how severe the consequences of successful cyberattacks have become.

With the deteriorating state of law and order in cyberspace, domestically and internationally, it is little wonder that significant corporate entities are no longer content limiting themselves to passive cybersecurity and are increasingly resorting to more aggressive forms of self-defense. This is reminiscent of the dynamics in earlier times and places where governments have proven unable to fulfill the fundamental social contract between modern states and their citizens and other entities under their jurisdiction. Typical of these situations is considerable legal ambiguity and fluidity regarding measures private entities can legitimately undertake in self-defense. Naturally, this state of affairs is far more acute when such dynamics are occurring in an increasingly interdependent and globalized international system. The quasi-anarchic nature of cyberspace further impedes quick fixes and other possible remedies.

Various private sector entities have been responding to this situation by developing, undertaking, or contracting out for a range of practices—some of them controversial—commonly referred to as active cyber defense (ACD).[2] Furthermore, numerous entrepreneurs scattered around the world have apparently been entering this field, offering their ACD services to corporations seeking such support. A gray market for relatively assertive, even aggressive, active cyber defense measures is burgeoning globally. Companies worldwide are contemplating and, in some cases, engaging in or contracting for practices of uncertain legality in the ACD domain.[3] Many are taking advantage of the ambiguous legislation and regulations on cyber activities in the United States, and even more amorphous ones in many other countries, to offer or employ ACD services.[4] Reluctance of governments to prosecute those involved in such activities even when they presumably violate current national laws only strengthens the incentive structure to contemplate such actions.

A gray market for relatively assertive, even aggressive, active cyber defense measures is burgeoning globally.

More assertive than passive defenses and other forms of cyber hygiene such as firewalls, ACD measures allow defenders to engage adversaries within and outside of the defender's networks. They may do so in order to gather intelligence, disrupt planned or ongoing attacks, attempt to reverse the damage from successful attacks, or (in extreme cases) punish attackers. There are diverse assessments of the ad hoc and systemic utility inherent in these practices. Yet it is clear that with the rapidly mounting costs and risks exacted by offensive attacks, the appeal of private sector ACD to complement basic passive security measures is hard to dismiss.

For some financial sector entities and others facing the most severe and persistent threats, such measures appear to be an especially attractive option. Yet this activity is occurring without much effective oversight and accountability, let alone international harmonization.

There are valid reasons to believe that ACD (excluding hacking back), if done professionally and responsibly, could prove a useful addition to the tool kit available to private sector entities to protect their key equities and minimize damages of attacks. Private sector ACD could even potentially benefit law enforcement, intelligence, and other national security agencies. Yet some ACD measures also have serious potential to cause collateral damage, escalation, and other unintended consequences for the defender and third parties, as well as adverse effects on certain other intelligence and law enforcement efforts. Such practice could also potentially carry systemic risks, were private companies to engage in vigilantism across national boundaries or even target foreign state actors. Yet there are mounting pressures, most evident in the United States, to further liberalize the restrictions banning or restricting some forms of ACD.[5]

The challenges in regulating private sector cyber activity reveal a fundamental friction between states' desires to monopolize cyber measures and the imperatives of the private sector to defend itself in a space where it has the capabilities, opportunities, and strong incentives to do so. This friction is not unique to the cyber domain; it is evident in analogous historical experiences. One recent instructive case is the rise of the private maritime security industry in response to piracy in the Gulf of Aden in the late 2000s, and the subsequent dilemmas it posed for governments trying to regulate the practice. This experience demonstrates the importance of legal and ethical debates over the desirable nature and extent of private sector self-defense, yet it also cautions against letting the irresolution of such debates paralyze practical efforts to shape norms of behavior that will otherwise be driven purely by dynamics of supply and demand.

This report explores the right balance between private sector ACD and state(s') ultimate responsibility to provide law and order, including in cyberspace. It discusses a limited spectrum of ACD practices that, if conducted within certain constraints and subject to some conditions, could prove a net positive, serving to minimize the risks and costs of cyber incidents facing companies without creating excessive harm. It examines ways to manage the potential consequences of private sector ACD, including revisiting domestic legal regimes governing ACD activity alongside mechanisms to harmonize these requirements internationally. The pitfalls inherent in unilateral state solutions, even in powerful and influential states such as the United States, are simply untenable. Creative mechanisms to regulate this activity globally will be crucial for the creation of legitimate space for private sector ACD.

The report begins by examining the characteristics of ACD practices—especially those emerging from the private sector—and the benefits and dilemmas they engender for governments and corporations. It then proceeds to (1) identify a spectrum of ACD measures (short of extreme practices like hacking back) that could strike the right balance between private

sector self-defense and state action in cyberspace; (2) propose generic principles to govern this activity; and (3) discuss an incentive structure and other mechanisms to promote adherence with and harmonization of these governing principles internationally. It is informed by an analysis of the challenges posed by private sector use of force in the maritime security industry and the mechanisms that evolved to mitigate risks and promote principled behavior among security providers.

THE SPECTRUM OF ACTIVE CYBER DEFENSE

The very term "active defense" commonly elicits visions of launching counterhacks against adversaries and, in certain circles, fosters strong objection to ACD as a legitimate private sector activity. However, in practice, the phenomenon is more nuanced. ACD includes a diverse range of cyber measures and practices from the relatively innocuous—such as setting up decoy targets in a defender's network—to more assertive measures that take place outside the defender's network but are nonetheless designed to frustrate incoming cyberattacks or mitigate their consequences.[6] The most extreme forms include highly offensive measures involving retaliatory, disruptive, or even destructive responses against the attacker. Moreover, ACD measures are not necessarily confined to the cyber domain and potentially involve other behaviors in the physical world designed to harass, disrupt, or punish cyberattacks. ACD may take different forms with varying consequences depending on whether conducted by governments or private companies.

There is no consensus on a definition of ACD encompassing the range of measures examined here. It is important to deduce the nuances of the technical nature and scope of ACD. Robert Dewar's definition provides several useful distinctions between ACD and other forms of passive cyber defenses:

> [A]n approach to achieving cyber security predicated upon the deployment of measures to detect, analyse, identify and mitigate threats to and from communications systems and networks in real-time, combined with the capability and resources

> to take proactive or offensive action against threats and threat entities including action in those entities' home networks.[7]

Various ACD measures may be employed preemptively, during an ongoing attack at various points along the "cyber kill-chain,"[8] and/or in the aftermath of an attack to reverse or mitigate damage. They can affect both the defender's networks and external networks and computers belonging to the attacker or an intermediary. Paul Rosenzweig offers a useful typology of ACD measures based on the types of effects they have on networks and computers—including observation, access, disruption, and destruction—and whether the actions are internal to the defender's network or external.[9] Rather than provide an exhaustive list of ACD measures, the following selection of less aggressive to more aggressive measures merely demonstrates the broad spectrum and characteristics of some of the best-known current techniques ascribed to ACD.

Less aggressive ACD measures that are typically taken within the defender's network include intrusion-prevention systems that detect hostile traffic and revise firewalls to block it. Deception techniques (for example, planting false data to disguise targets or creating entire decoy networks) make it difficult for the attacker to access the desired information. "Honeypots" or "honeynets" lure the attacker into an isolated system through a deliberate vulnerability, preventing access to other areas. "Sandboxes" or "tarpits" provide barriers that slow or halt and examine incoming traffic that may be suspicious. And various means of intelligence gathering, including in the "dark net," can collect information on cyber threats inside and outside one's systems.[10]

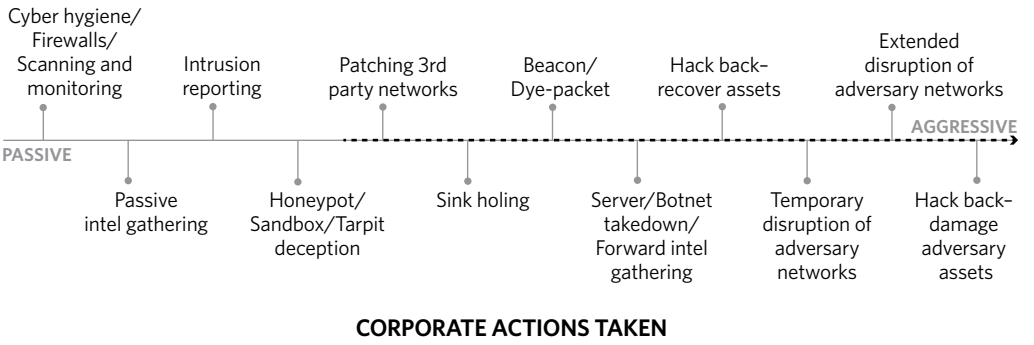
More aggressive measures that typically access and alter third-party networks include "sinkholing," which redirects malicious traffic to a system under control of the defender, and "patching" vulnerabilities in a third party's hijacked computer. Measures analogous to LoJack recovery systems or "digital dye-packets" allow the defender to track data exfiltrated from its network. "Digital beacons" or watermarks similarly alert the defender when stolen data resurfaces elsewhere. Defenders can also temporarily disrupt the servers the attacker relies on or dismantle botnets, which use networks of infected machines to launch attacks.

Finally, the most aggressive actions include forward intelligence gathering (including in external networks and systems) to collect evidence or information about the attacker (for example, capturing their image through their webcam). "Hack backs" into the attacker's networks can retrieve, alter, or erase stolen data. The attacker's own systems can be disrupted temporarily to impede their ability to launch attacks or over an extended duration (for example, by locking down a computer). Most controversially, hack backs could even damage the attacker's networks or computers to prevent further loss or punish the attacker.

The grouping of these measures is a necessary simplification—individual measures could be conducted in more or less aggressive ways or in combination with others. For instance, a honeypot could be used to launch measures with disruptive impacts on the attacker's systems.[11]

The degree to which a particular ACD measure is considered aggressive depends on a number of dimensions. In addition to Rosenzweig's typology of effects and the degree to which measures affect external networks, other factors include the profile of the targets (unwitting participants in an attack, innocent third parties, or adversary networks); the temporal nature of effects (temporary, extended, or permanent) and their scope (localized or broader); and the degree to which the ACD measures are automatic and autonomous. Naturally these dimensions do not always correlate, but it is possible to place common measures on a spectrum according to how aggressive they are (see Figure 1 for a visual representation).

Figure 1. **Spectrum of Cyber Defense**



Note: Carnegie's participation in the George Washington University Center for Cyber and Homeland Security's Active Defense Task Force included a briefing of an early version of this spectrum approach. The task force adopts a similar model in *Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats.*

The black dashed line in Figure 1 indicates approximately where measures begin to generate effects outside of the defender's network. However, the distinction between internal and external is often blurred; some measures may be deployed and/or directed at the target in the defender's network but still have the potential (and even intent) to affect external networks. Further, even the boundary between networks is disputable.[12]

ADVANTAGES AND RISKS OF ACTIVE CYBER DEFENSE

Active cyber defense serves as a potential complement, rather than alternative, to passive cyber defense. When responsibly undertaken, ACD can enhance cybersecurity by offering

unique functions, or advantages, to the defender (as well as some strategic systemic benefits) that passive defenses do not. Some ACD measures, however, carry inherent risks that will vary depending on the capacity of the defender and the threat. The advantages and liabilities appear at both the tactical and broader strategic levels (see Table 1).

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

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

ACTIVE CYBER DEFENSE AS A CYBERSECURITY STRATEGY

Active cyber defense is not a purely technical phenomenon, and its merits and drawbacks must be weighed in the context within which ACD measures are or could be conducted. Given the lack of clarity around roles and responsibilities for private sector defense, it is pertinent to distinguish how and toward what ends governments and private actors could conduct ACD.

The first distinction is the function that ACD measures are designed to serve:

- Gathering intelligence on threats and assisting with attribution;

- protecting assets within the defender's network;
- disrupting imminent and ongoing attacks;
- imposing costs directly or indirectly on the adversary;
- denying gains by tracing and recovering assets that have been exfiltrated;
- blocking or disabling attack vectors, and complicating attack planning; and
- preventing future attacks by inhibiting the adversary's capabilities or by diminishing the appeal of future attacks (deterrence by denial).

Taken together, these functions represent a broad strategy toward cybersecurity predicated upon altering the calculus of malicious actors through reshaping the environment and corresponding incentive structure in which they operate. In this sense, the functions of government and private sector ACD are not mutually exclusive, but they can be distinguished in several ways.

Active cyber defense, as a conceptual approach to cybersecurity, can be compared to a concept in criminology known as Situational Crime Prevention (SCP).[13] SCP focuses on altering the settings that provide opportunities and incentives for crimes rather than focusing on the criminals per se. This is done through a wide range of actions to increase the effort required and risks associated with committing a crime, reduce rewards, and mitigate the situational factors that provoke criminals or provide excuses for crime. Critically, this includes not just efforts via the criminal justice system but also efforts via public and private organizations that manage and shape the environment in which criminals operate. Thus, SCP does not depend on eliminating criminal threats or changing the motives of criminals. Because this approach focuses on environmental and circumstantial factors, the benefits of such efforts often extend to both those targeted and those not targeted that also occupy that environment.[14]

As in the SCP case, government and private sector ACD offer distinct opportunities to combat malicious activity in cyberspace—each of which could potentially produce positive externalities. Governments may employ ACD for a wider set of functions, including defense of "friendly" systems and networks under their authority and in combination with other activities inside or outside of cyberspace. While governments may undertake activities that are punitive in nature (including law enforcement action), such activities reside outside any conceivable legitimate scope of permissible private sector ACD.

However, major companies that shape the environment of cyberspace will inevitably play a more salient role in protecting it. This is in part because increasing reliance on cloud-based

services and the interconnection of devices, among other trends, are raising the potential for a major cyberattack to cause cascading effects. As stated in a 2016 World Economic Forum white paper, "it is an understatement to say that the government and industry are struggling to understand and prepare for the magnitude of systemic cyber risk."[15]

The functions or roles of government and the private sector also differ on a procedural level—in terms of the authority under which an activity is conducted and the degree of consent to potential actions affecting third parties. Governments undertake ACD under a broad mandate in the law enforcement, homeland security, intelligence, and military contexts. The authority of private sector ACD, insofar as it affects third parties, may be derived from a company's end-user license agreement or digital rights management protocols or procedures. In other cases, private sector ACD may be conducted with cooperation and oversight by governments or under the authority of a court order. This authority directly pertains to the legitimacy of private sector ACD. Generally speaking, the legitimacy of private sector engagement in ACD becomes more contentious as it moves across the scale toward more aggressive acts, particularly when crossing from internal to external network actions.

The debate over private sector ACD is not merely whether to allow companies to conduct a certain set of technical activities. At the broadest level, it is about the respective roles and contributions of the government and private sector in cybersecurity in managing systemic risk and how ACD could or should fit into these. Both the technical and contextual dimensions are relevant in considering the desirable scope, conditions, and procedures surrounding the conduct of ACD in the private sector. Selective private sector ACD could be harnessed in a situational approach to shaping this dynamic environment to decrease the opportunities and incentives for malicious activity. The benefits of doing so would extend beyond the immediate companies conducting ACD to the broader public reliant on their services and vulnerable to systemic risks.

THE CASE FOR PRIVATE SECTOR ACTIVE CYBER DEFENSE

Globally, as well as domestically in the United States, the private sector is currently suffering from critical gaps in cybersecurity. At one level, there are "nuisance" cyberattacks that companies can mitigate through adequate cyber hygiene and passive defense, such as firewalls and routine scanning and monitoring. At a higher level are sophisticated, criminal and state-sponsored (and hybrid) cyberattacks on companies on the scale of national security threats, which governments are inclined to address through their own means (both cyber and noncyber). Between these levels are the increasingly sophisticated, targeted cyberattacks that governments cannot (or will not) take action to mitigate but that exceed the ability of passive defenses to prevent.

The imperative of all forms of defense—passive and active, governmental and private—is especially acute as current commercial and technical trends concentrate ever larger amounts of critical assets in the cloud, away from their physical corporate spaces and owned and operated by a handful of cloud service providers.

Yet governments have limited resources and personnel to thoroughly protect against, investigate, and respond to cyberattacks. These resources are already strained by the primary responsibility of defending government systems and networks. In some cases, governments might not be able to match the private sector's capacity to respond to attacks. Even if governments could muster the capacity to adequately defend the private sector, companies may not want government agencies to have the degree of access to and control over their networks and data needed

to defend them. From a broader perspective, it may not be desirable to use public resources to protect private companies, particularly if it has the effect of driving down the incentive for companies to spend scarce resources to protect themselves (in other words, a moral hazard).

The borderless nature of cyberspace raises further legal and ethical questions for governments. Should the state accept responsibility for defending networks and computers of its companies that lie outside of its territory? Should it defend those of foreign-owned companies or multinational corporations located within its territory? Should it extend its defense to cloud-based assets? States pursuing such strategies will inevitably face dilemmas regarding who and what to prioritize and how far to go in their defense.

Internationally, the role of governments in defending private entities varies greatly. Some states assume significant responsibility for cybersecurity of the private sector (including ACD), while others reserve the right to intervene only when absolutely necessary, such as in the defense of critical infrastructure. The leeway that states give to the private sector to engage in ACD similarly varies and is evolving. Yet considerable state responsibility for defense of the private sector may become untenable, even for countries where this is currently the norm. The expansion of companies' vulnerabilities due to, among other factors, increasing standardization of products, the exponential growth of the Internet of Things,[16] and tremendous reliance on cloud-based and remote access services will motivate businesses to fill gaps in the defensive coverage that governments provide. Furthermore, the onus of responding to cyberattacks is already emerging as a tall order for governments because of the difficult policy choices associated with any type of response or inaction against the perpetrators, even in situations where they can be confidently identified.

The unevenness of the international regulatory environment exacerbates the dilemma that many governments face. They can try to maintain a monopoly on legitimate engagement in ACD—despite their limited ability to deliver on it and to regulate a growing international market for ACD services—or they can step aside and allow companies to engage in activities with the substantial risks described above.

Should governments try to restrict the space for private sector ACD without offering a credible alternative to protect the interests of corporations, they risk incentivizing corporations to relocate resources to environments more hospitable to freedom of action or to avail themselves of the ACD services offered offshore. On the other hand, an overly permissive environment risks engendering a "race to the bottom," when companies begin relying on cheaper, less experienced, or more reckless contractors within the international market for ACD services.

RISING DEMAND FOR PRIVATE SECTOR ACD

In the absence of effective defense provided by governments or other credible means for risk management against acute cyber threats, key actors in the private sector are increasingly eager and willing to develop and employ their own means of self-defense through ACD. A growing industry of cybersecurity providers advertises services including honeypots and other more innocuous forms of ACD.[17] These companies' ACD services are part of a much larger, rapidly expanding cybersecurity industry that some expect to reach $175 billion in value by the end of 2017 (compared to $78 billion in 2015).[18] There are numerous cases of companies involved in the dismantling of botnets with varying degrees of law enforcement collaboration, including the recent effort by INTERPOL and several cybersecurity companies to dismantle the Simda botnet, which infected computers in more than 190 countries.[19]

Key actors in the private sector are increasingly eager and willing to develop and employ their own means of self-defense through ACD.

Beneath the surface exists a much more extensive gray market, offering services of uncertain legality. Assessing the scope of these activities is difficult, and much of the evidence is anecdotal. A survey in 2012 at the Black Hat USA security conference found that 36 percent of respondents claimed to have engaged in retaliatory hacking.[20] Many companies overcome their own reluctance to engage in ACD by outsourcing their ACD services at home or abroad. In 2013, the Federal Bureau of Investigation allegedly investigated whether U.S. financial institutions hired hackers to disable servers that Iran used to launch attacks the previous year.[21] Some cybersecurity companies reportedly have entire divisions located abroad to engage in activites they would not legally be able to engage in the United States.[22]

Facing the most severe and persistent threats, the financial sector seems to have clear motives for pursuing more aggressive measures to defend against cyberattacks. As one former military intelligence officer put it, "Banks have an appetite now to strike back. . . . if the government can't act, or won't, it's only logical they'll do it themselves."[23] Dennis Broeders describes the vibrant "stealth market" in the Netherlands for banks and other financial sector entities to hire companies, including those based abroad, to take down the servers of their attackers.[24] This market operates under the radar, across national boundaries, and with little to no oversight. The inability of governments to protect the private sector has generated what Dutch National Prosecutor for Cybercrime & Lawful Intercept Lodewijk van Zwieten describes as "a whole industry waiting in the wings to take over that role."[25]

While it is difficult to determine the full extent of these practices, a revealing trend is that of some governments toward tacitly or even explicitly embracing private sector ACD. For in-

stance, in its *National Cyber Security Strategy 2016–2021*, the UK government has stated it "will draw on its capabilities and those of industry to develop and apply active cyber defence measures to significantly enhance the levels of cybersecurity across UK networks."[26] The scope of activities this entails and freedom given to private companies remain to be seen. Singapore appears to have gone the furthest toward facilitating private sector ACD, albeit with a unique arrangement for official sanction. A 2014 amendment to the country's Computer Misuse Act created what Craig et al. describe as "a mechanism for state-sanctioned active defense to protect critical national infrastructure," which potentially even includes in certain cases "preemptive strikes against perceived cyber threats."[27]

The desire of many for the cybersecurity industry to have greater leeway to conduct even the more aggressive forms of defense is manifested in increasing calls in the United States and elsewhere for changes to laws preventing companies from engaging in ACD. For instance, in 2013, *The IP Commission Report* recommended that companies engage in techniques to track data stolen from their networks in a cyberattack or even lock down the computer of an unauthorized user trying to access it.[28] More recently, the 2015 annual report to Congress by the U.S.-China Economic and Security Review Commission called for Congress to "assess the coverage of U.S. law to determine whether U.S.-based companies that have been hacked should be allowed to engage in counterintrusions for the purpose of recovering, erasing, or altering stolen data in offending computer networks."[29]

Yet the desire to unshackle the private sector needs to be tempered by an understanding of the risks and consequences if ACD practices spread without corresponding development of sound principles and an incentive structure to encourage their responsible use.

RISKS AND BENEFITS OF CREATING SPACE FOR LEGITIMATE PRIVATE SECTOR ACD

RISKS

An overly permissive environment for private sector engagement of ACD could result in the conduct of ACD by ill-equipped defenders, as well as potentially systemic destabilizing effects.

Interference in law enforcement activity and unintended political consequences. There are substantial risks to international stability that could materialize from unregulated private sector ACD. Widespread use of aggressive measures by private companies could complicate efforts by law enforcement and militaries to clearly delineate legitimate from criminal activity or national security threats. Companies could even accidentally interfere with the activities of an intelligence, homeland security, or law enforcement agency from their own state

when engaging an attacker. The greatest concern would be the potential for an international crisis caused by an escalating exchange of cyberattacks and counterhacks between companies in two states or a company that, wittingly or unwittingly, targets another state's intelligence or military. For example, a sequence of increasingly destructive hack backs between a U.S. company and a Chinese (potentially state-owned) company could quickly become an international incident and prompt both governments to intervene.

Greater exposure due to unnecessary risk taking and lack of capacity. Many successful cyberattacks on companies could have been prevented simply through adequate passive defenses and other sound risk management practices. There is a real concern that in the absence of effective governing principles, creating a more permissive legal environment for ACD will encourage companies to resort to unnecessary risky behavior in lieu of investing in cyber hygiene or possibly more cumbersome measures to minimize exposure. Moreover, only some companies have the sophisticated capabilities and personnel to effectively manage the middle to high-end ACD operations and contain the risks of collateral damage. Those that lack resources to conduct sophisticated effective defense might do more harm than good to themselves and to third parties. It is often difficult for the defender to fully assess the capabilities of the attacker, and thus, the defender could risk escalation with a potentially superior or more risk-inclined adversary that might even spill over to the physical world.[30]

Complicated management due to varying laws across countries. Finally, there are significant legal concerns with the use of private sector ACD. International law does not provide much clarity on how private sector self-defense in cyberspace should and would be treated.[31] National laws in some countries prohibit ACD practices by the private sector entirely. However, laws, including those in the United States, are often ambiguous or even amorphous regarding the permissibility of many types of ACD short of the extreme cases.[32] Presumably, in many cases, ACD that damages or even accesses a computer in another country could violate the domestic laws in that country, and therefore, the defender would be subject to legal ramifications in that country.[33] Serious extradition issues for aggressive ACD perpetrators might arise as well, especially between friendly states.[34]

BENEFITS

The risks of private sector ACD are real and significant but not unmanageable. Many are contingent on the circumstances and parameters in which ACD is conducted. These risks must be weighed against the potential benefits from an environment conducive to private sector engagement in certain ACD measures.

Reduced burden on government, allowing for more targeted resource use. Even minimal private sector ACD can play a role in assisting law enforcement to tackle cyber threats

through gathering intelligence and tracking malicious actors. Enabling the private sector to better defend its networks through ACD could spare governments some of the resource and policy burdens of responding to many cyberattacks on the private sector and allow them to focus on more persistent threats to their nations. Filling a critical gap below the threshold that necessitates state intervention on behalf of the private sector could ameliorate a major source of tension between states.

Faster response time and improved effectiveness. Often, the private sector can react faster and more effectively to defend its own networks than governmental homeland security or law enforcement agencies can. Individual corporations likely have a better picture of the unique threats they face and the risks they pose to their equities than governments. They have a stronger motivation to defend themselves and, in some cases, they also possess superior technical and financial resources to allocate to that mission. The aforementioned benefits of ACD as a complement to passive defense could thus be more efficiently realized if the private sector itself is enabled to undertake it rather than shackled legally and hamstrung by governmental insistence that they refrain from action prior to consultation with governments and/or courts. Finally, ACD conducted to gather intelligence on attribution would give the private sector a tool to enable law enforcement action on its behalf—comparable to the role private investigators of intellectual property or insurance fraud crimes regularly play in assisting law enforcement prosecution.

Systemic long-term improvements to cybersecurity. Empowering the private sector to engage in certain ACD measures could considerably improve the cybersecurity landscape. ACD could limit the potential for any single vulnerability to become an aggregated risk that compromises a large number of systems: individual systems would be less dependent on the innate security of a potentially vulnerable product or service. This concern will only increase along with the use of cloud-based and remote access services. Reducing the likelihood of cascading effects could in turn positively impact insurability against cyber risk by diminishing the aggregation of risks. Additionally, by increasing the legitimate or accepted ability of the private sector to deny benefits and raise costs to hackers, ACD could have a cumulative effect of deterring malicious activity by reducing the expected payoff of cyberattacks. Even those entities not conducting ACD would benefit from this deterrent effect, as attackers could not be certain of defenders' capabilities.

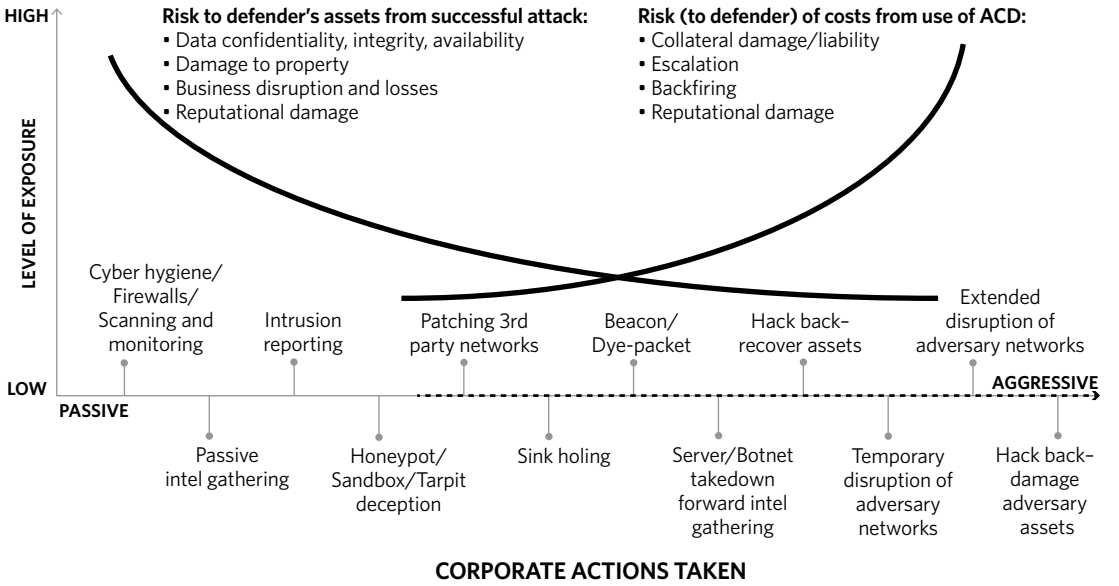
IDENTIFYING A SPECTRUM OF NET-BENEFICIAL ACD

Private sector ACD demands a more nuanced approach to evaluating the conditions under which the risks would be minimized and the gains could be realized. These conditions include the scope of activities conducted and the parameters placed upon their conduct.

Viewed from the private sector perspective, ACD involves an inherent tradeoff between two broad categories of exposure to risk. The first includes the costs and consequences of suffering from a successful cyberattack, including the immediate loss of confidentiality, integrity, or availability of data, intellectual property, and critical services, as well as the less direct (but no less worrisome) costs such as reputational damage. The second includes the potential costs and consequences of defensive actions taken by the company. These could include collateral damage (or excessive damage), escalation, backfiring, or other unanticipated effects. Moving across the spectrum of aggressive ACD may decrease the former category of risks, whether by preventing, mitigating, recovering from, or deterring future cyberattacks. However, resorting to more aggressive measures—particularly once they begin to have effects outside of the defender's networks—may increase the latter category of risks and liabilities. Chart 2 roughly illustrates how a corporation's decisions to move toward more aggressive ACD measures may affect its risk exposure.

Private sector ACD demands a more nuanced approach to evaluating the conditions under which the risks would be minimized and the gains could be realized.

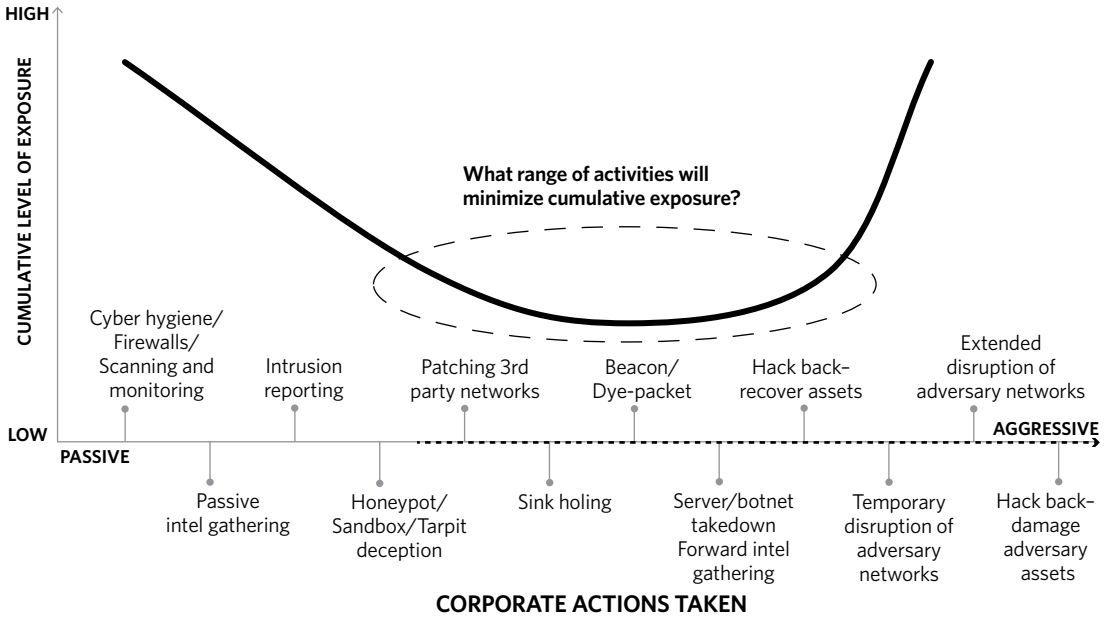
Figure 2. **Balancing Corporate Cyber Risks**



Note that the location and shape of these curves do not reflect a definitive technical judgment; they are merely offered for illustrative purposes. No single ACD measure is guaranteed to decrease the risk of a corporation being hacked. How this graph would look in reality for a particular corporation will depend on its unique threat environment, capabilities, and choices in the use of ACD. The specific types of cyberattacks a company is defending against determine the feasible response options. As in other domains, these responses to cyberattacks are not limited to the domain of cyberspace and could include actions in the physical world, such as tracking down and exposing the attacker's or its sponsor's identity or engaging with law enforcement in the attacker's state. Thus, Figure 2 is intended to reflect the general impact of employment of ACD.

If these two types of risk are combined and the impact of ACD on the cumulative exposure of the corporation is weighed, it may be possible to identify a limited spectrum of ACD—excluding inordinately risky activities like hacking back—that could serve to minimize the cumulative exposure of the corporation. These activities would rest between those that are already commonplace and largely uncontroversial on the one hand and those that carry outsized risk and should be ruled out entirely on the other. The area in between would consist of those practices that, if conducted within a widely accepted framework of principles and in a circumscribed manner by competent operators, could serve not only to benefit the corporations employing them but also potentially the broader objective of maintaining stability of the international system (see Figure 3).

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



Again, this chart is merely for illustrative purposes. Completely elucidating a spectrum of activities that would minimize exposure is beyond the objectives of this report. Doing so would require capabilities such as those of the insurance industry to analyze and quantify these risks. The spectrum here is laid out primarily to understand the ACD measures being discussed as a basis for a principles-based approach.

Accepting that there is a spectrum of active cyber defenses that, if conducted in a principled manner by competent actors, has the potential to improve not only the fortunes of individual players but also the current cybersecurity situation writ large still leaves open a question: How can those electing to engage in active cyber defense be motivated to operate within such bounds? Here it is useful to examine the experience of maritime security to understand the factors leading to the rise of private use of force, the challenge it posed for governments, and the mechanisms for promoting standards and preventing a race to the bottom in the industry.

INSIGHTS FROM MARITIME SECURITY

In the mid-2000s, a breakdown in governance in Somalia created a breeding ground for pirates in the Gulf of Aden. The pirates' methods evolved from simply boarding and stealing from ships to hijacking and holding entire ships and their crews hostage. The average ransom for a large commercial vessel reached $4 million by 2010, and some estimate the total cost of such an attack (including the ransom and prolonged detention of ship, cargo, and crew) to be as high as $20 million.[35]

This deteriorating security environment in a critical region for global shipping provided the immediate catalyst for the shipping industry's adoption of private armed security contractors. A deeper analysis of the conditions that gave rise to this unique solution yields insights into the interacting pressures that drive industry behavior and the struggles of governments in attempting to manage these forces.

Upon eventual recognition of the problem, governments proceeded to deal with the rising threat from piracy by deploying naval power to the Gulf of Aden and Indian Ocean. But they found their resources strained by the ever-growing scope of the problem, compounded by the daunting policy and legal challenges associated with adopting a more aggressive attitude toward piracy or taking action against a host state beset by chronic ungovernability. Despite individual and multinational naval forces amounting to ten separate naval fleets operating in the region, the number of reported pirate attacks in the high-risk area increased about 300

percent from early 2008 to early 2009.[36] The difficulty in distinguishing pirates from the thousands of legitimate fishermen operating in the vast area contributed to this challenge—naval forces tried to deter and intervene in ongoing attacks instead of taking a more proactive approach. Conflicting rules of engagement practiced by the various navies involved in joint efforts further undermined effectiveness. Few of the warships present were actually interdicting suspected pirates.[37]

According to David Axe, "the unworkable military solution combined with legal limits on ship self-defense" resulted in an environment conducive to exploitation by pirates.[38] Shipowners (and their insurers) were thus presented with the painful choice of either risking a protracted detention of ships, crew, and cargo or paying millions of dollars to the pirates to free them all and, in the process, making the piracy business even more lucrative. Oceans Beyond Piracy estimated that the total economic cost of piracy in the Western Indian Ocean—including direct costs from attacks, costs of naval operations and other mitigation measures, and other indirect costs—reached at least $7 billion by 2010, while the number of seafarers taken hostage that year was 1,090.[39]

THE RISE OF PRIVATE MARITIME SECURITY AND DILEMMAS OF GOVERNANCE

Shipping companies had no practical options for avoiding the high-risk and globally important area. Though they experimented with some passive defenses, such as safe rooms and even unarmed guards, these proved insufficient to stem the growing threat. Companies began to turn to private armed guards, stimulating rapid growth of the industry of private maritime security contractors (PMSCs). The proportion of ships transiting the high-risk area protected by armed guards increased from around 10 percent in 2009 to 27 percent in 2010.[40] Insurance was relatively quick to embrace the practice. In October 2009, a leading global insurance broker, Marsh, began offering a 50 percent discount on insurance for ships hiring RedFour, a PMSC.[41] Though many governments did not approve of the practice, most either lacked explicit prohibitions on the employment of private armed guards on commercial ships or proved reluctant to enforce them, thereby paving the way for companies to hire contractors without official oversight.[42]

Governments faced a fundamental dilemma—they wanted to maintain a monopoly on the use of force but, in many cases, had neither the capability nor willingness to fulfill the demand for defense against piracy. Nor did many governments have practical options to dissuade the private sector from taking on this role itself. As the demand for armed guards rose, governments faced no other realistic option than to accept it, implicitly if not explicitly. The German government, for instance, openly admitted in 2011 that the overwhelming demand

from the private sector for state protection onboard their vessels pushed it to reverse policy on the issue of private armed guards.[43] It struggled to implement a system for certification that would allow it to retain some form of control, but the gap in governance had already grown under its hesitation. As a result, as Burgin and Schneider state, "the demand for security on behalf of German ship owners meant that, until the implementation of a licensing procedure, unlicensed PMSCs were employed out of necessity."[44]

The decision to allow PMSCs confronted states with a number of subsequent issues, including whether to allow ships to contract PMSCs from other countries or only its own nationals; the specific areas in which PMSCs were allowed to operate and carry weapons; the requirements for vetting and licensing companies or even individual personnel; and the types of armaments that were allowed and procedures for their storage and transfer. Beyond logistical and procedural considerations, there were also serious decisions with regard to defining the rules of engagement, bounding defensive actions that were legitimate for PMSCs, and dealing with situations when those boundaries were crossed.[45]

Individual states varied widely in their answers to these questions and approaches to regulations. An uneven regulatory environment motivated the use of "flags of convenience," whereby ships could relatively easily avoid burdensome regulations by sailing under the flag of a state with more relaxed rules.[46] Other attempts to avoid regulations included hiring escort ships when contractors were not allowed to board ships directly and the use of "floating armories"—ships that would hold weapons and equipment in international waters for contractors to pick up before missions—to circumvent national restrictions on arms transfers through ports. "Thousands of weapons pass through the Indian Ocean and hundreds of security teams rotate on and off ships in the Gulf of Oman" that largely operate in an unregulated space.[47] These practices led to international incidents, including one in 2013 when Indian authorities seized a floating armory owned by a U.S. company that had drifted into its territorial waters and subsequently imprisoned the thirty-five men on board.[48]

Without effective regulations or accountability at the national level, let alone international level, some companies relied on guards who lacked sufficient training and engaged in reckless behavior. A retired U.S. merchant marine captain, James Staples, called it the "Wild Wild West," saying "there are no regulations or vetting process for these teams. The company doesn't know who it's getting on board. There's no training requirement or training for lifesaving."[49] Michelle Bockmann and Alan Katz said that the industry was at risk of a "Blackwater moment:"

> Fear of pirate attacks is creating more violent and chaotic seas, where some overzealous or untrained guards are shooting indiscriminately, killing pirates and sometimes innocent fishermen before verifying the threat, according to more than two dozen interviews with lawyers, ship owner groups, insurance underwriters and maritime security companies.[50]

PROFESSIONALIZATION OF THE INDUSTRY

David Isenberg warned in 2012 of incentives for a race to the bottom and stated that "all elements of the maritime industry want a code of conduct for the use of force and a clear legal structure for the provision of security."[51] Yet this race was forestalled in part through a combination of pressures within the industry. Two developments occurred in 2011: the first case of a major maritime insurer issuing public guidance for shipping companies on the employment of PMSCs and the establishment of the Security Association of the Maritime Industry (SAMI).[52] Launched in May 2011, SAMI would eventually include 180 members from thirty-five countries and was praised by many for promoting standards that improved the industry's practices—including for the use of floating armories and use of force by contractors to prevent collateral damage or unnecessary escalation.

As industry associations and insurance embraced the practice, they drove professional standards in the industry, such as hiring personnel with military training. SAMI worked with Marsh to develop a comprehensive insurance package specifically for the industry. This further promoted professionalization by offering members of the association preferred rates.[53] SAMI eventually served as the basis for industry standards including ISO 28007 and the 100 Series Rules for the Use of Force.[54] Further evidence of the effectiveness of these industry-driven standards is their incorporation into policy; for instance, the United Kingdom now includes certification under ISO 28007 in its voluntary approach toward regulation of PMSCs.[55]

As industry associations and insurance embraced the private sector practice, they drove professional standards in the industry, such as hiring personnel with military training.

Rapid expansion of the maritime security industry corresponded with a substantial decrease in piracy. By the end of 2011, nearly half of the ships transiting the high-risk area were protected by PMSCs, according to some estimates.[56] While the number of attempted hijackings by Somali pirates increased, the success rate of hijackings decreased from 27 percent in 2010 to 13 percent in 2011.[57] From 2011 to 2012, the number of reported *attempted* attacks in the area decreased from 237 to 75, indicating that the plummeting success rate was likely deterring future attacks from being attempted.[58] This dramatic decrease is attributable to several factors, including the presence of naval forces, PMSCs, and other deterrence measures taken by ships. But notably, the period of greatest decline in attacks coincided with the largest increase in total expenditures on PMSCs—around 80 percent between 2011 and 2012.[59]

The impact of armed guards on piracy in the Gulf of Aden and Indian Ocean is particularly evident in comparison to the Gulf of Guinea and Southeast Asia where restrictions in ter-

ritorial waters prevent the use of PMSCs and where piracy is more prevalent.[60] Attacks by Somali pirates in the Gulf of Aden declined from a peak of 237 in 2011 to zero in 2015 and only two attempts in 2016.[61] Oceans Beyond Piracy estimates that the total economic costs of piracy in the region decreased from $7 billion in 2010 to $1.4 billion in 2015.[62]

KEY TAKEAWAYS FOR PRIVATE SECTOR ACD

In the maritime security experience, norms and practice regarding the private sector use of force were driven less by deliberate decisions by governments than by economic imperatives. Historically, this has been the case since maritime privateering began in the thirteenth century—tacitly or sometimes explicitly embraced by governments. This early experience offers its own relevant insights for cybersecurity, which are discussed more extensively elsewhere.[63] In the case of modern norms regarding arming private commercial vessels, it is telling that many in the shipping industry were initially just as averse to bringing arms onto ships as regulators, believing it would lead to escalation or other liabilities. Writing around the peak of the crisis in 2012, Berube and Cullen stated:

> Although in the past commercial shipping associations and trade unions have been adamant that keeping the sea lanes safe and open for commerce is the exclusive job for states and have been reluctant to accept the additional costs and liability associated with armed self-protection, for the first time in over a century, this is now changing.[64]

Within a relatively short time span, norms evolved and major industry associations switched their policy positions and more or less endorsed the use of PMSCs. The economic imperatives of individual companies catalyzed a shift in industry behavior, which in turn led to changes in governmental policies—albeit not evenly so—across the globe.

From the evidence available, it seems that, if anything, vulnerable private sector entities are more predisposed toward ACD than the shipping industry was toward armed contractors. Well-established and codified maritime traditions had placed restraints upon the deployment and employment of firearms aboard commercial vessels. Norms regarding private use of force in cyberspace are far less solidified and will likely be more ephemeral than in the maritime case due to the constant evolution of technology and practice. However, the maritime security experience also suggests that it may be possible to develop and incentivize common principles and standards for the use of active cyber defenses that could begin to alleviate the concerns surrounding their use. In considering such an approach, there are six important takeaways from the maritime security analogy.

1. **When lawlessness prevails and governmental action is weak and ineffective, private entities facing existential threats will tend to fend for themselves.** The private sector will turn to its own means of self-defense to compensate for insufficient government action. The underwhelming track record of law enforcement (as well as other state efforts) globally to check the escalation of cyberattacks undermines the case for prohibiting key players in the private sector from enhancing their self-defense capabilities and actions.

2. **A tradeoff of risks is inescapable.** In the case of ACD, some degree of risk will be inevitable, but it may be possible to develop practices and standards to minimize those risks to an acceptable level. This seems likely given that the risks of ACD are certainly less contentious and far more innocuous in comparison to the risks that the use of firearms in maritime security posed to human life. Employing armed guards on ships carried its own risks, but over time, the assurance provided by industry-driven standards, such as practices for vetting personnel and rules of engagement, made this an easier calculation.

3. **The limited control of governments over the domain, especially internationally, offers opportunities for the private sector to circumvent regulations for the sake of effectiveness.** Government authority and control in cyberspace is attenuated in ways similar to the maritime domain. It is inherently difficult to police the actions of companies in cyberspace, and, even if it were somehow to become easier, options remain to relocate one's ICT assets and/or outsource activities to countries with a more permissive atmosphere. For these reasons, any policy approach must begin with the international context and try to anticipate how various national choices impact the international market of services.

4. **Fears that private sector action will lead to a systematic escalation of the problem are largely unfounded or at least overstated.** Evidenced by the maritime security experience, private sector activities can increase the costs to attackers, thereby helping to deter future attacks and contribute to a long-term descalation in aggressive measures. Concerns that pirates would respond to armed guards by resorting more rapidly to violence and using more lethal weapons such as rocket-propelled grenades and machine guns were a significant source of resistance to PMSCs.[65] But, in actuality, their employment corresponded with a dramatic decrease in the human costs of piracy, including the number of seafarers attacked with firearms.[66] Of course, the presence of armed guards at sea initially led to incidents of violent confrontation and death that might otherwise not have occurred. But the overall risks of escalation even at the tactical level proved manageable by professionalization of the practice and the promulgation of balanced rules of engagement that guided proportionate responses to threats, such as signaling and firing warning shots. These were incorporated into industry practice—for example,

being inserted into the International Maritime Organization guidance issued in September 2011, which recommended employment of an "accurate and graduated level of deterrence, at a distance."[67] Likewise, limitations on the types of weapons that PMSCs could use helped reduce the risk of systemic escalation. The convergence of the industry around such principles was essential to mitigate the escalation risks arising from employment of PMSCs.

Turning to the cyber domain, the potential for systemic escalation to more aggressive behavior and tactical escalation in the context of individual engagements requires vigilance when it comes to ACD, whether conducted by governments or the private sector. However, one cannot assume that in the absence of evidence, employment of ACD will inevitably provoke wanton escalation. More importantly, these risks can be managed by two complementary approaches: First, a systemic shift toward increasingly destructive exchanges can be prevented by constraining the spectrum of legitimate activities to exclude those that prove inordinately risky (for example, destructive hack backs)—bearing in mind that unlike the maritime piracy domain, no use of lethal means is even under consideration. Second, the risks of escalation within the context of a particular engagement can be managed via principles (analogous to the rules of engagement) that guide behavior for those activities.

5. **Incentives will drive buy-in and adherence to norms and best practices.** Key stakeholders motivated to minimize risk—the shipping and insurance industries—drove professionalization and best practices among PMSCs. Insurance, in particular, proved to be an appealing and effective mechanism for risk management because it could directly manipulate the economic incentives that were shaping industry behavior. This suggests that an attractive way to incentivize ACD providers to adhere to norms is indirectly through leveraging key stakeholders' interest in seeking to minimize cybersecurity risk—stakeholders such as the financial and energy sectors, major ICT companies, and insurance providers.

6. **Stopgap measures may not solve the problem permanently but will allow a more stable environment to develop.** Armed guards were a stopgap measure rather than a solution to the problem of piracy. Indeed, as a result of shipping companies and antipiracy forces letting down their guard over the past few years, there has been a gradual resurgence in Somali piracy—with the first successful hijacking in March 2017 of a large commercial vessel since 2012.[68] While the underlying factors fueling piracy remain, Phillip Cable, chief executive officer of Maritime Asset Security & Training, states that the deterrent effect of security forces is "keeping it at bay."[69] Notably, this resurgence has led senior U.S. military officials to encourage shipowners to redeploy security measures.[70] There were policy and legal ambiguities regarding the employ-

ment of PMSCs that went unresolved, but, nevertheless, they provided a much-needed reprieve to the private sector in the midst of a crisis. Likewise, ACD may not promise to solve the challenges of cybersecurity, but it may offer a remedy en route to a more stable environment. Moreover, PMSCs did not create an irreversible loss in state control over the use of force as subsequent efforts to develop certification mechanisms demonstrated. Arguably, the success of PMSCs in ameliorating the crisis gave governments more time to develop effective regulations.

LIMITS OF THE ANALOGY

Analogies always have limitations, and the maritime piracy analogy to cyberattacks is no exception. The dilemmas of ACD are more complex in certain respects than maritime security. While attribution challenges in cyberspace can be similar to the challenge of distinguishing a pirate from a fishing vessel, one problem that was not present in maritime security situation in the late-2000s (at least to the same degree) was the challenge of malicious state activity targeting private entities. Had a naval ship attacked a commercial oil tanker, it would likely have been immediately clear that it was not a pirate attack. Private companies suffering from cyberattack, however, may not be able to immediately discern the actor attacking it or its motives, raising the possibility that ACD could be used against another state's security or military forces unintentionally. This outcome is not necessarily unequivocally negative from the perspective of deterring malicious activity at a systemic level, given the circumscribed nature of ACD responses discussed here (especially compared to a PMSC firing at a suspected pirate). The possibility that a cyberattack might be a state or state-sponsored actor with considerable capabilities nevertheless complicates the task of determining the risk of any response.

Pirates in the Gulf of Aden were relatively predictable because they were driven by roughly the same motivation: economics. When the costs rose and expected benefits of attempted hijackings decreased, attempts in turn decreased. Malicious cyber actors motivated by geopolitical objectives, however, may have a far different calculus than cybercriminals, which affects whether and how they can be deterred.

Finally, geography still played a defining role in how the maritime security industry evolved. While the pirate activity eventually covered a huge geographic area, it was still relatively clear over time when companies were operating in the high-risk areas and when they were not. The immediate effects of a company's self-defense action, including use of force, were limited in scope to a local area and thus the impacts were far easier to discern. A malicious attacker and defender in cyberspace may be operating in different states with different national laws. The cyberattack and the defensive response could, in turn, affect third parties in

other states. Moreover, the physical components and systems that comprise the infrastructure of the Internet lie within states' legal authority, and thus, actions traversing and affecting these systems do not occur in an environment outside of national legal jurisdictions like the high seas.

In any case, differences between maritime and cyber domains do not negate the analogy's value, particularly for understanding the dynamic interaction between the threat environment, government regulation, and private sector norms and practice, as well as private sector mechanisms for incentivizing principled behavior.

Private maritime security filled a critical gap in protection of the private sector in the midst of a crisis. Rather than a standalone solution, PMSCs constitute one leg of what Peter Cook, former chief executive officer of SAMI, describes as a "three-legged stool"—the combination of armed guards, best practices for security measures taken by companies short of armed force, and international naval forces to manage the most severe threats.[71] The UK security company Control Risks emphasized the combination of these three factors as contributing to a 90 percent reduction in incidents of piracy between 2012 and 2013.[72] The systemic impact this had in deterring piracy served to benefit even those companies that did not employ armed guards themselves; with increasing uncertainty of the defensive capabilities of targets, the expected payoff of piracy attacks on any target *potentially* employing PMSCs decreased. Private sector ACD has the potential to serve a similar function in a deteriorating cybersecurity environment for many industries. The importance of this analogy, however, is not simply in illustrating this role but in elucidating how the private sector's ability to perform that role successfully hinges on its understanding and observing the key constraining factors.

A PRINCIPLES-BASED APPROACH TO PRIVATE SECTOR ACD

In the case of private maritime security, a focus on governance came after the private sector more or less had already embraced the practice. This may also be the case with ACD, given the apparent growth of activity in this domain. The current state of play with regard to private sector ACD suggests that, as soon as possible, those looking to constructively manage the practice should develop realistic principles and incentivize industry to comply with them rather than try to promulgate and enforce an ineffectual ban. This is especially important given that these activities are likely to continue to expand internationally as both the potential capabilities and demand for better security increase.

Those looking to constructively manage the practice should develop realistic principles and incentivize industry to comply with them rather than try to promulgate and enforce an ineffectual ban.

The potential benefits make it highly desirable, if not unavoidable, to systematically open more opportunities for the private sector to engage in ACD internationally. At the same time, doing so necessitates first bounding the spectrum of private sector ACD to those measures that would minimize cumulative exposure to a company (excluding such practices as hacking back) as demonstrated in Figure 3. The conduct of these activities should then be guided by internationally agreed-upon norms and principles. Private sector ACD should not be viewed as an either-or choice. A menu of legitimate ACD practices should be approached

cautiously and revised based on experience. The movement of a defender along the spectrum toward more aggressive activities should be contingent on its capabilities to meet principles and other requirements set forth.

The principles should aim to delineate norms of behavior to bound the parameters and guide the conduct of private sector ACD. They would not legitimize risky or unlawful activities, but rather realistically define risk-minimizing conduct. Examining what such conduct might look like in the ideal (yet feasible) international environment entails looking beyond the current legal and policy regime. Even if there were a consensus on interpretation of the law in the United States or elsewhere that precluded ACD, such laws are subject to amendment, as many have advocated elsewhere.[73] Although there is a rich and fascinating (if ultimately inconclusive) debate about the ethics, legality, and expediency of private sector ACD,[74] the legal ambiguities surrounding ACD should be set aside here in order to foster constructive analysis of the practice and ways to manage it.

NORMATIVE PRINCIPLES FOR THE CONDUCT OF ACD

The following list of principles have the potential to promote these goals and gain broad support from both those desiring to engage in ACD and those concerned over its potential negative consequences. Some of them are clearly inspired by principles of international law, including law of armed conflict, but such frameworks are of only limited applicability to nonstate actors and to cases below the threshold of use of force. Thus, unique principles are needed for the ACD context. These principles could serve as a platform for the convergence of various approaches by the cybersecurity industry, insurers, governments, and other stakeholders over rules and practices regarding this area of activity. They do not constitute a definitive or exclusive list, and instead are intended to serve as a starting point.[75]

Purpose: ACD measures should be conducted with a predetermined objective. Objectives may fall under one or more of these functions: to gather intelligence on threats; protect critical corporate assets, including data, physical property, and critical services; deny benefits to the attacker; and diminish the incentives for future attacks. ACD could also be used wherever possible to assist law enforcement actions against malicious actors. ACD should never be used for retribution, retaliation, or vigilantism, or for commercial gain against competitors.

Scope and duration: ACD measures should be conducted within the minimum scope required and cease upon attainment of the predetermined objective. Some capabilities would only be allowed while attacks are unfolding or ongoing and should cease at the end of the attack (in other words, not continue to control the adversary's network). Others could

potentially be used in the immediate aftermath of an attack (for example, beacons). ACD measures with extended duration would be legitimate only against persistent threats.

Necessity: ACD measures should only be employed to complement the other options available for defending or mitigating the damage from cyberattacks. ACD should be confined to those measures necessary to stop attacks and reverse their damage. They should be principally directed at the perpetrator of the attacks but might have to include highly limited and time-bound effects against third-party networks through which attacks are routed.

Proportionality: The potential adverse side effects of ACD must be commensurate with the immediate benefits. The measures must produce effects that are localized and preferably temporary and/or reversible.

Effects: ACD measures should be designed with safeguards against causing collateral damage, such as an inability to self-propagate or self-replicate. Measures should only be used if they are tested, well understood, and sufficiently controlled. Activities resulting in excessive damage or destruction should be off limits.

Oversight: ACD practitioners should commit to operating by these principles and submit to ad hoc oversight when conducting out-of-network ACD operations. Established procedures for accreditation of those providing or engaging in ACD are desirable, but they could be developed by private sector entities and not necessarily through governmental regulation.

Sharing: ACD practitioners should share best practices and experiences with their peers and cooperate on efforts, whenever possible and as relevant. Given necessary antitrust restrictions and the imperatives of protecting information sensitive for commercial and security reasons, those engaging in ACD should be encouraged to work together to the extent possible. This will further the collective benefits accruing from ACD and diminish the prospects for mistakes in its application.

Collaboration: ACD practitioners should be encouraged to collaborate with law enforcement in managing major cyber threats, bearing in mind the unique sensitivities and requirements for the protection of information. ACD practitioners should inform and cooperate with law enforcement agencies (and, if need be, homeland security) in ongoing attacks and subsequent investigations.

Accountability: ACD practitioners should keep records of their practices to be able to justify, should the need arise, the necessity and proportionality of their responses. When ACD measures could impact the external networks through which attacks are being routed, efforts should be taken to alert and cooperate with third parties before taking those measures. If time-sensitive measures preclude this, then they should be alerted after the response. At the

operational level, there should be a clear chain of command within the defender's organization that places decisions to carry out certain actions with the proper senior authorities. Automation should be prohibited for capabilities with potentially damaging or disruptive effects outside the defender's network.

Liability: The defender should be liable for damage and/or the disruption of legitimate services it causes to innocent third parties. There could be liability for damages inflicted on the attacker if the ACD measures prove excessive or punitive in nature or were abused for commercial advantage. If damage or disruption occur as a direct result of an ACD measure, the defender should be responsible for proving that it acted in self-defense and out of necessity and that it took appropriate means to diminish these. The requirements for minimizing risks will scale up depending on the scope of the activity undertaken and the capacity of the defender. Practices carrying significant risk would entail increasingly onerous requirements and may assume liability too great for any but the most advanced defenders.

Discretion: Whereas the above principles are intended to be universally applicable, the conduct of ACD may be subject to the additional and unique requirements and conditions that different governments may choose to apply. Based on their unique circumstances and governance and legal traditions, states may impose their own requirements, standards, or prohibitions at their discretion, which those under their jurisdiction would then have to comply with.

IMPLEMENTATION OF PRINCIPLES FOR ACD

Looking ahead, it appears that, broadly speaking, private sector use of ACD could move in one of two directions. The first is greater government regulation and/or monopolization of capabilities, with little to no private sector ACD permitted. The second is a sort of "Wild West" scenario where the government steps back and private sector entities engage in ACD at their will. Both of these paths have drawbacks and risks that have been detailed elsewhere.[76]

An internationally harmonized approach to managing private sector ACD will be necessary, among other reasons because of the potential extradition issues that may arise from the conduct of ACD by private entities.

National laws, regulations, and norms will not be sufficient in such a globalized domain. An internationally harmonized approach to managing private sector ACD will be necessary, among other reasons because of the potential extradition issues that may arise from the conduct of ACD by private entities. Yet achieving consensus on a global treaty to regulate this space would require strenuous and

time-consuming efforts, if it is attainable at all. Even if a treaty were arrived at, it would be difficult to enforce and too rigid to adjust to changing circumstances. There needs to be an exploration of other institutional arrangements for codifying the objectives and principles that should guide private sector ACD.

There are other ways to anchor ACD practices in the above principles. One option would be to embed the principles in national standards and regulations for companies wishing to engage in ACD. Governments could take a cautious approach to allowing a certain level of ACD activity, while imposing constraints and requirements upon the companies engaging in it. These could include registration, certification or accreditation, limits on the capabilities companies are allowed to employ, best practices, requirements for oversight, and appropriate cooperation with law enforcement. Governments could also elect to deputize, on a selective basis, those wishing to engage in ACD in a manner akin to Singapore's approach, as was occasionally done in other domains where governments by themselves proved unable to impose law and order. However, many of these requirements might face serious push-back from the private sector and would not overcome the inherent limitations of a national regulatory approach to manage evolving practices, particularly in the growing international market of services.

In the absence of common principles, states moving in different policy directions at varying speeds may intensify friction throughout the international system. Of greater concern is the possibility that uneven approaches would only serve to disadvantage those attempting to promote norms of restraint and reward those who disregard them. Alternatively, excessive national restrictions could encourage corporations to relocate their assets and operations to more promiscuous jurisdictions. Companies in the United States and elsewhere already face a competitive disadvantage in certain respects by laws limiting ACD. Countries may be hesitant to agree to similar restraints in this space if they believe their companies benefit from the lack thereof.

For these reasons, a better option may be to emulate the model of industry-driven standards seen in the private maritime security case. This approach would seek to promote a legitimate international market for ACD services, limited to those activities that would minimize cumulative exposure and conducted with appropriate constraints, conditions, and accountability.

One mechanism for doing so could be a corporate social responsibility (CSR) initiative embedded in an industry association similar to SAMI, serving as a means of self-governance by the industry. Or, alternatively, an institution could be modeled after the International Code of Conduct (ICoC) for Private Security Service Providers, a multistakeholder initiative led by the Swiss government that created a voluntary set of rules to govern practices of private security contractors ranging from vetting and hiring practices to rules of engagement and

protection of human rights.[77] Finalized in 2010, the ICoC was successful in gaining commitments from more than 700 companies in a wide range of states within three years. A voluntary code of conduct could be developed to govern the conduct of ACD, and adherence in this case would be incentivized via similar market mechanisms that have been successful in the case of the ICoC. A specific proposal is outlined in more detail in the Appendix.

Whatever the mechanism, the process of institutionalizing these principles could benefit from building upon existing areas of international agreement such as the Budapest Convention, an international treaty relating to cybercrime adopted by the Council of Europe in 2001 and ratified by fifty-five states since.[78] The process for developing international private sector standards could be an independent initiative or an offshoot of existing fora, such as the Internet Governance Forum, G7, or International Telecommunications Union.

The insurance industry can function as the most adroit incentivizer and steward of effective risk reduction.

Such efforts will be critical in gaining the acceptance of governments of a principles-based initiative. But equally important to its success will be bringing together the key segments of the private sector that comprise the potential providers, users, and insurers of ACD activities. Coordinating these stakeholders in a manner similar to how SAMI worked with the shipping and insurance industries to regulate security providers could be an effective mechanism for promoting principles for ACD.

THE ROLE OF THE INSURANCE INDUSTRY

The insurance industry could play a crucial role in the promulgation of principles for private sector ACD.[79] Only the insurance industry is capable of achieving near-perfect insight of all the information critical to successful ACD. Through the underwriting process, it gains knowledge of deployed controls, processes, and capabilities. Through the claims process, it understands causes of loss, what parties were involved, and what the costs were. Because most insurance policies are reviewed annually, it also stays up to date on industry developments. Finally, because most companies buy insurance, it has the ability to compare relative risk management postures and maturities across industries. When this information potential is achieved, as can be exemplified best by the maritime example, the insurance industry can function as the most adroit incentivizer and steward of effective risk reduction.

Specifically, the normal functioning of the insurance industry can allow it to play a critical role in both identifying and incentivizing the most effective and appropriate ACD principles and practices, predicated on the companies' requisite maturity to utilize ACD in the

first place—for example, the technical ability to carry out measures. More importantly, companies would first have to demonstrate the ability to tackle fundamental cyber hygiene. Firms that do exhibit such requisite maturity would have the benefit of insurance coverage for any incidental losses and accidental collateral damage resultant from the ACD measures. This dynamic ultimately becomes cyclical and expansive in nature: the insurance industry continually expands its knowledge of ACD practices, thus allowing it to continually define the ACD spectrum; premiums and available coverage are adjudicated according to the relative risk profiles and ACD maturity of each company. At a minimum, an interim step could be to employ ACD via a specialized maturity model that ties the level of ACD that might be practiced to the fulfillment of various criteria for corporate maturity. Over time, the insurance industry would disperse this continually refined knowledge to new companies that gain the capability to use ACD (with the insurance industry's help).

Also inherent in this dynamic is the insurance industry's ability to disincentivize inappropriate behavior by either charging hefty premiums for activities that are extraordinarily risky or not underwriting certain ACD practices that are either illegal or immoral.

The key to unlocking this potential is data sharing and proof of concept. Simply put, the insurance industry needs to gain an understanding of what ACD looks like in practice and, ideally, needs access to a cost-benefit analysis of successful measures. This can only happen if companies that successfully utilize ACD embrace the potential power of the insurance industry and exhibit a willingness to share information beyond basic cyber hygiene practices. In turn, the insurance industry must become receptive to taking more risk than that which is encompassed by the currently available cadre of cyber insurance products. If these goals are achieved, there is no reason why the insurance industry cannot serve as a primary driving force of successful ACD utilization and the resulting reduction in cyber risk.

CONCLUSION

Cyberspace remains an environment conducive to malicious activity. The increasingly offense-dominant nature of this domain may lead to a tipping point, as Jason Healey warns, where the Internet "would no longer be merely the Wild West, but a failed state like Somalia."[80] It is more necessary than ever to consider not just the present state of private sector ACD but how the practice will evolve under intensifying pressure from malicious actors.

There are a number of reasons to expect the trends fueling demand for private sector ACD services to accelerate. Capabilities for both malicious and defensive activity will likely evolve at a faster rate than regulations can adapt. Vulnerabilities will proliferate at an ever greater rate with the Internet of Things, and this will in turn increase the costs and externalities of cyber incidents. Law enforcement resources may be spread increasingly thin. Even more worrisome is the potential for further escalation of the severity of cyberattacks. Should there be a shift toward cyberattacks targeting the integrity of data, the consequences could become even more damaging and cascading than anything seen before.

There already exists a vibrant international market for private sector ACD services, governed by questionable ethics and lacking any real oversight. The maritime security experience offers an admonition against waiting until a prohibition on activity has become untenable to try and impose norms. This analogy also challenges a prevailing assumption in many discussions about ACD that any approach needs to begin with either changes to existing law or work within its

confines. Rather than a top-down approach, norms and standards created within the industry of PMSCs evolved over time into policy. The boundaries between legitimate and illegitimate activity are not defined solely by regulations—they are a product of the interaction of evolving threats, technological innovations, market dynamics, and governmental interference.

If governed by effective principles that can achieve some degree of international consensus, the practice of private sector ACD as a complement to passive measures could substantially improve private sector defense and alter the calculus of malicious actors—even if practiced selectively as in the case of armed guards in the maritime context. This principles-based approach is centered on minimizing cumulative risks—looking holistically at the impact of ACD on exposure rather than focusing narrowly on the risks or pitfalls of a single technique or capability.

Efforts toward relaxing or otherwise modifying legal restrictions pertaining to private sector ACD are not desirable until more information becomes available on the efficacy of various ACD measures and the viability of principled conduct by the private sector.

This demands a cautious, evolutionary approach to private sector ACD informed by experience of its utility and consequences to ensure that the right balance between state authority and private sector self-defense. Allowing a certain level of private sector engagement in ACD does not necessarily entail an irrevocable loss of state authority. However, efforts toward relaxing or otherwise modifying legal restrictions pertaining to private sector ACD are not desirable until more information becomes available on the efficacy of various ACD measures and the viability of principled conduct by the private sector. As in the case of maritime security, adjustments can be made as experience reveals the most effective and appropriate roles for governments and the private sector, respectively.

Such an effort need not be viewed as a permanent solution to either the challenges of cybersecurity or governance of private sector activity. It is unlikely to resolve all of the complex legal and policy clashes or broader normative disagreements among states. However, as the maritime security experience demonstrates, doing so may not be necessary to achieve the immediate objectives of promoting positive industry behavior and harnessing the potential of ACD while minimizing its potential detrimental effects.

APPENDIX: INTERNATIONAL CODE OF CONDUCT FOR PRIVATE SECTOR ACTIVE CYBER DEFENSE

Consonant with the need to consider international approaches to promoting norms for the conduct of ACD, the below proposal outlines how the aforementioned principles could be anchored in a voluntary, international code of conduct (CoC) for private entities engaging in ACD. This proposal envisions a collaborative multistakeholder process—including representatives from relevant industries, civil society, and governments—for developing the CoC internationally. Such a process could be modeled after that of the International Code of Conduct for Private Security Service Providers or other CSR initiatives.

The CoC's core would be built around the principles described above. The objective would be to define the spectrum of legitimate ACD practices that would minimize cumulative exposure and provide a framework for the conduct of practices within that spectrum by private entities in a manner that manages their risks. This framework could do so by placing constraints and requirements on practices commensurate with the risks of engaging in them. The most innocuous defenses would face few, if any constraints. ACD impacting external networks would be circumscribed and conducted with appropriate national (law enforcement) oversight. Destructive hack backs would be prohibited entirely.

The CoC would encourage and incentivize companies to take lower-risk measures first before resorting to more aggressive measures. Some activities could have associated technical requirements—for instance, digital dye-packets should be thoroughly tested and designed to prevent

unanticipated effects. Companies would also have to demonstrate a clear imperative to move up the scale of effects and to take actions outside their networks. Unnecessarily risky measures would be ruled out.

Participants in the CoC would not be required to conduct any ACD, but would agree to remain within the bounds of legitimate ACD practices defined by the CoC. Beyond simply agreeing to principles, participants could establish a platform serving a number of purposes, including providing a forum for companies to share information on best practices, an avenue to update and adapt the CoC to evolving technology and practice, and an independent mechanism for oversight and accountability. This could potentially include a variety of other elements:

- An internal certification process (of personnel or technical capabilities);
- technical requirements for capabilities, such as built-in safeguards to prevent ACD capabilities from disrupting unintended networks;
- specific constraints and requirements on some forms of autonomous ACD, for instance requirements for testing and certification and limits on the types of capabilities and degree of automation;
- information sharing on cyber threats, possibly through a dialogue among members; and
- recognition of companies meeting best practices and standards.

HALLMARKS OF THIS APPROACH

The CoC would be inherently flexible, allowing it to keep pace with the market dynamics and changing technology. The CoC would be designed to surmount some of the barriers that limit the ability of governments to circumscribe ACD through national regulation—including the international market for services that allows companies to outsource these capabilities and enlist "hackers for hire." Likewise, it would be designed to be more attainable than binding international agreements or mechanisms. The CoC could

- Serve as an interim step en route to more ambitious norms developed or codified in this domain;
- build momentum slowly as more companies and states adhere to it rather than needing immediate buy-in from all (granted, a quorum will likely be needed); and
- adapt to evolving technology and practices faster than approaches through regulation or legally binding mechanisms.

Conversely, compared to deregulation in the absence of norms in this space, the CoC could help positively shape the market for these services. The CoC would

- Promote professional standards for professional cybersecurity providers, which could further reduce the risks that individual operators cause collateral damage or escalation;
- reduce incentives that drive black or gray markets for capabilities and services by creating a more legitimate practice of ACD; and
- discourage vigilantism by companies or individuals.

IMPLEMENTATION AND INCENTIVIZING ADHERENCE

The CoC should serve to incentivize best practices in the market (rather than strictly regulate it) by creating a standard for the legitimate practice for those companies that wish to engage in ACD. Incentives to join could include, but are not limited to, the following:

- Market access—institutions that hire the services of private cybersecurity companies could require membership in the CoC as a condition for contracts.
- Improved capacity—the CoC could be an effective conduit for information sharing on threats within the cybersecurity industry internationally and membership would be required for participating in any such arrangements. This increased cooperation could dramatically improve the ability of the industry to stay ahead of emerging threats.
- Public-private cooperation—individual governments could require entities to adhere to the CoC in order to be able to engage in operations like botnet takedowns.
- Insurance coverage and competitive advantage—as discussed above, the insurance industry could play an essential role in supporting the CoC, and critically, in defining the spectrum of ACD practices that would minimize cumulative exposure of a company by analyzing the risks and potential gains associated with particular measures. Insurance companies could operationalize this in defining those intentional acts that would void coverage. Membership in the CoC itself could affect premiums paid by companies; for instance, a bank hiring a cybersecurity provider would have a direct economic incentive to hire one within the CoC.
- Reputational benefits—if widely accepted, membership in the CoC would be a clear indicator that the cybersecurity provider maintains the best standards and

practices in the industry. Certification requirements set up within the CoC would be another assurance of the provider's capabilities. These reputational benefits would extend to those companies receiving ACD services by signaling that they are taking strenuous measures to ensure the security of their own and their clients' assets and insuring the risks associated with them. This could even help offset the reputational damage of a successful breach (if one were to nevertheless occur) by demonstrating that it was not simply a result of negligence or lack of effort to enhance cybersecurity.

Participation in the CoC would not prevent a company from legally engaging in any activity that a nonmember could—those practices the CoC might rule out would likely be illegal in any event. It could, however, provide confidence that the company meets the highest standards and best practices when conducting such activity. While it is unlikely to eliminate the black or gray markets of hacking services and tools, the CoC could create a more legitimate market for these services, which industries and governments could turn to with greater confidence.

NOTES

1 Lily Hay Newman, "What We Know About Friday's Massive East Coast Internet Outage," *Wired*, October 21, 2016, https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/.

2 The term active cyber defense is used throughout this report merely because it has become the term of choice for referencing employment of a broad set of technical capabilities and activities for cyber risk and damage mitigation. While it is an imprecise and perhaps loaded term—in part because it is often associated with one extreme form of active defense (hacking back)—none of the other available terms to refer to the same phenomenon are any more definitive. Active cyber defense as used here is not synonymous with hacking back.

3 Michael Riley and Jordan Robertson, "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.

4 Dennis Broeders, "Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance," Netherlands Defence Academy, 2015.

5 For instance, Representative Tom Graves (R-GA) has recently circulated a comprehensive proposal for legislation to amend the Computer Fraud and Abuse Act to allow for limited ACD measures; see, Active Cyber Defense Certainty Act [Discussion Draft], 115th Cong., 2017, https://tomgraves.house.gov/uploadedfiles/discussion_draft_ac-dc_act.pdf. See also, "Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats," Center for Cyber and Homeland Security, October 2016, https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf.

6 In this report, the term cyberattack refers broadly to operations in cyberspace that attempt to compromise or impair the confidentiality, availability, or integrity of electronic information, information systems, services, or networks.

7 Robert Dewar, "The 'Triptych of Cyber Security': A Classification of Active Cyber Defence" (6th Annual Conference on Cyber Conflict, 2014), NATO Cooperative Cyber Defense Center of Excellence, https://ccdcoe.org/cycon/2014/proceedings/d1r1s9_dewar.pdf.

8 For a description of this concept, see Irving Lachow, "Active Cyber Defense: A Framework for Policymakers," Center for New American Security, February 22, 2013, https://www.cnas.org/publications/reports/active-cyber-defense-a-framework-for-policymakers.
9 Paul Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures," *Stanford Journal of International Law* 50, no. 1 (Winter 2014): 2.
10 For more extensive discussion on methods and the role of intelligence gathering, see, "Into the Gray Zone," Center for Cyber and Homeland Security.
11 Karine Bannelier and Theodore Christakis, "Cyber-Attacks Prevention-Reactions: The Role of States and Private Actors," *Les Cahiers de la Revue Défense Nationale*, 2017.
12 Rosenzweig, "International Law."
13 For an introduction to this concept, see, Martha Smith, "Situational Crime Prevention," Oxford Bibliographies, last updated April 14, 2011, http://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0040.xml.
14 Ibid.
15 Global Agenda Council on Risk and Resilience, "Understanding Systemic Cyber Risk," World Economic Forum, October 2016, http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf.
16 Internet of Things (IoT) refers generally to the increasing interconnectedness and connection to the Internet of a vast range of devices, including such things as household appliances. According to one estimate, the global economic impact of IoT could be between $3.9 and $11.1 trillion by 2025. See, Global Agenda Council on Risk and Resilience, "Understanding Systemic Cyber Risk."
17 Amanda N. Craig, Scott J. Shackelford, and Janine S. Hiller, "Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis," *American Business Law Journal* 52, no. 4 (Winter 2015).
18 Alec Ross, "Want Job Security? Try Online Security," *Wired*, April 25, 2016, http://www.wired.co.uk/article/job-security-cybersecurity-alec-ross.
19 "INTERPOL Coordinates Global Operation to Take Down Simda Botnet," press release, INTERPOL, April 13, 2015, https://www.interpol.int/News-and-media/News/2015/N2015-038.
20 Craig Timberg, Ellen Nakashima, and Danielle Douglas-Gabriel, "Cyberattacks Trigger Talk of 'Hacking Back,'" *Washington Post*, October 9, 2014, https://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-of-hacking-back/2014/10/09/6f0b7a24-4f02-11e4-8c24-487e92bc997b_story.html.
21 See Michael Riley and Jordan Robertson "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.
22 Ibid.
23 Shane Harris, *@War: The Rise of the Military-Internet Complex* (New York: Houghton Mifflin Harcourt Publishing, 2014), 119–20.
24 Broeders, "Investigating the Place and Role of the Armed Forces," 43.
25 Ibid.
26 "National Cyber Security Strategy 2016–2021," UK Government, 2016, 12.
27 Craig, Shackelford, and Hiller, "Proactive Cybersecurity."
28 Commission on the Theft of American Intellectual Property, "The IP Commission Report," National Bureau of Asian Research, May 2013, 564.
29 "2015 Annual Report to Congress," U.S.-China Economic and Security Review Commission, November 2015, 33.
30 Jan Kallberg, "A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs," *IT Professional* 17, no. 1 (January/February 2015).
31 Rosenzweig, "International Law."

32 In the United States, this includes, most importantly, the Computer Fraud and Abuse Act (18 USC 1030), which prohibits accessing any computer without authorization. For further discussion of the applicability to ACD, see Appendix II of "Into the Gray Zone," Center for Cyber and Homeland Security.
33 For a comparison of various states' laws prohibiting unauthorized access of another computer, see Craig, Shackelford, and Hiller, "Proactive Cybersecurity."
34 Paul Rosenzweig, Steven Bucci, and David Inserra, "Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense," Heritage Foundation, May 5, 2017, http://report.heritage.org/bg3188.
35 Anna Bowden and Shikha Basnet, "The Economic Cost of Somali Piracy, 2011," Oceans Beyond Piracy, 2012, http://oceansbeyondpiracy.org/sites/default/files/attachments/ECOP%20Full%20Report%202011.pdf.
36 David Axe, "Why the Somali Pirates Are Winning," *Guardian*, April 9, 2009, http://www.theguardian.com/commentisfree/cifamerica/2009/apr/09/piracy-somalia-alabama-us-navy.
37 Claude Berube and Patrick Cullen, *Maritime Private Security: Market Responses to Piracy, Terrorism and Waterborne Security Risks in the 21st Century* (New York: Routledge, 2012), 76.
38 David Axe, "Pirate-Fighters, Inc.: How Mercenaries Became Ships' Best Defense," *Wired*, August, 23, 2011, https://www.wired.com/2011/08/pirate-fighters-inc/.
39 Matthew R. Walje et al., "The State of Maritime Piracy 2014: Assessing the Economic and Human Cost," Oceans Beyond Piracy, 2014, http://oceansbeyondpiracy.org/publications/state-maritime-piracy-2014.
40 Simon O. Williams, "The Development and International Regulation of Private Maritime Security," Tactique Ltd., November 2014, http://www.kcl.ac.uk/sspp/departments/dsd/research/researchcentres/StrategyandPolicy/corbett/Tactique-Briefing---The-Development-and-International-Regulation-of-Private-Maritime-Security.pdf.
41 Berube and Cullen. *Maritime Private* Security, 34.
42 Carolin Liss, "(Re)Establishing Control? Flag State Regulation of Antipiracy PMSCs," *Ocean Development & International Law* 46, no. 2 (2015): 84–97.
43 Berube and Cullen, *Maritime Private Security*, 6.
44 Annina Bürgin and Patricia Schneider, "Regulation of Private Maritime Security Companies in Germany and Spain: A Comparative Study," *Ocean Development & International* Law 46, no. 2 (2015): 123–37.
45 For further discussion of these questions, see Liss, "(Re)Establishing Control?"
46 Berube and Cullen, *Maritime Private* Security, 82.
47 Sarah Kent and Cassie Werber, "How Floating Armories Help Guard Cargo Ships From Pirates on High Seas," *Wall Street Journal*, February 3, 2015, http://www.wsj.com/articles/how-floating-armories-help-guard-cargo-ships-from-pirates-on-high-seas-1422934573.
48 Cassie Werber, "The Capture of a Floating Armory and Its Crew Reveals a Strange Industry on the High Seas," *Quartz*, January 14, 2016, http://qz.com/593272/the-capture-of-a-floating-armory-and-its-crew-reveals-a-strange-industry-on-the-high-seas/.
49 Michelle Wiese Bockmann and Alan Katz, "Shooting to Kill Pirates Risks Blackwater Moment," Bloomberg, May 8, 2012, http://www.bloomberg.com/news/articles/2012-05-08/shooting-to-kill-pirates-risks-blackwater-moment.
50 Ibid.
51 David Isenberg, "The Rise of Private Maritime Security Companies," *Huffington Post*, July 29, 2012, http://www.huffingtonpost.com/david-isenberg/private-military-contractors_b_1548523.html.
52 Berube and Cullen, *Maritime Private Security*, 5.
53 Mark Lowe, "Marsh Launch New Insurance Facility," *Maritime Security Review*, February 21, 2012, http://www.marsecreview.com/2012/02/marsh-launch-new-insurance-facility/.

54 "The Security Association for the Maritime Industry (SAMI) Announces Voluntary Liquidation," Maritime Cyprus, April 19, 2016, https://maritimecyprus.com/2016/04/19/the-security-association-for-the-maritime-industry-sami-announces-voluntary-liquidation/.

55 Nelleke van Amstel, "The ICoC and Regulation of Private Maritime Security Companies" (report on a meeting held in Geneva, July 2014), Geneva Center for the Democratic Control of Armed Forces, 2014.

56 Bowden and Basnet, "The Economic Cost of Somali Piracy, 2011."

57 Ibid. The number of attacks reported by year varies according to source. For example, the European Union Naval Force (Atalanta) reported twenty-five successful hijackings out of 176 attacks in 2011, while the International Maritime Organization reported thirty-three hijackings out of 286 attacks. Regardless of the range, all data show a decline in the success rate. See "Key Facts and Figures," European Union Naval Force Somalia, http://eunavfor.eu/key-facts-and-figures/; and "Reports on Acts of Piracy and Armed Robbery Against Ships: Annual Report 2011," International Maritime Organization, March 2012, http://www.imo.org/en/OurWork/Security/PiracyArmedRobbery/Reports/Documents/180_Annual2011.pdf.

58 "Piracy Falls in 2012, but Seas Off East and West Africa Remain Dangerous, Says IMB," press release, International Maritime Bureau, January 16, 2013, https://www.icc-ccs.org/news/836-piracy-falls-in-2012-but-seas-off-east-and-west-africa-remain-dangerous-says-imb.

59 Jonathan Bellish, "The Economic Cost of Somali Piracy, 2012," Oceans Beyond Piracy, 2013, http://oceansbeyondpiracy.org/sites/default/files/attachments/View%20Full%20Report_3.pdf.

60 Rob Lenihan, "Pirate Attacks on Ships Decrease as Companies Increase Security," *Business Insurance*, February 6, 2017, http://www.businessinsurance.com/article/20170206/NEWS06/912311752/Pirate-attacks-companies-increase-ships-security-International-Maritime-.Bureau?utm_campaign=BI20170208CurrentIssue&utm_medium=email&utm_source=ActiveCampaign.

61 Katharine Houreld, "Somali Pirates Hijack First Commercial Ship Since 2012," Reuters, March 14, 2017, http://www.reuters.com/article/us-somalia-hijack-idUSKBN16L0EW.

62 "The State of Maritime Piracy 2015: Assessing the Economic and Human Cost. 2015," Oceans Beyond Piracy, 2015, http://oceansbeyondpiracy.org/publications/state-maritime-piracy-2015; Walje et al., "The State of Maritime Piracy 2014."

63 See Florian Egloff, "Cybersecurity and the Age of Privateering," in *Understanding Cyber Conflict: 14 Essays*, eds. Ariel E. Levite and George Perkovich (Washington, DC: Georgetown University Press, 2017).

64 Berube and Cullen, *Maritime Private Security*, 4.

65 Small Arms Survey, *Small Arms Survey 2012: Moving Targets* (New York: Cambridge University Press, 2012).

66 Walje et al., "The State of Maritime Piracy 2014."

67 International Maritime Organization. "Revised Interim Guidance to Shipowners, Ship Operators, and Shipmasters on the Use of Privately Contracted Armed Security Personnel on Board Ships in the High Risk Area," International Maritime Organization, September 16, 2011.

68 Jason Patinkin, "Somalia's Pirates Are Back in Business," *Foreign Policy*, April 9, 2017, http://foreignpolicy.com/2017/04/09/somalias-pirates-are-back-in-business/.

69 Lenihan, "Pirate Attacks on Ships Decrease."

70 Helene Cooper, "Pentagon Warns Ships as Pirates Again Prowl Waters Off Somalia," *New York Times*, April 23, 2017, https://www.nytimes.com/2017/04/23/world/africa/james-mattis-somalia-pirates-djibouti.html.

71 Lenihan, "Pirate Attacks on Ships Decrease."

72 "RiskMap Report 2014," Control Risks Group Limited, 2013, https://www.controlrisks.com/webcasts/studio/flipping-book/riskmap-report-2014/riskmap-report-2014.html.

73 For a more extensive discussion of the legality of ACD and applicable legal analogies, see "The Hackback Debate," *Steptoe Cyberblog*, November 2, 2012, http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/; for suggestions on potential regulatory actions, see "Into the Gray Zone," Center for Cyber and Homeland Security.

74 See, for instance, Patrick Lin, "Ethics of Hacking Back: Six Arguments From Armed Conflict to Zombies" (paper prepared for the Ethics + Emerging Sciences Group, California Polytechnic State University), September 26, 2016, http://ethics.calpoly.edu/hackingback.pdf.

75 Other scholars have taken a similar approach. See for instance, Dorothy E. Denning, "Framework and Principles for Active Cyber Defense," *Computers & Security* 40 (2013).

76 For arguments on the limits of government regulation and need for private sector ACD, see Juan Zarate, "The Cyber Financial Wars on the Horizon: The Convergence of Financial and Cyber Warfare and the Need for a 21st Century National Security Response," Foundation for Defense of Democracies, July 2015; and "The IP Report," National Bureau of Asian Research; for arguments against allowing private sector ACD, see Kallberg, "A Right to Cybercounter Strikes"; and James Lewis, "Private Retaliation in Cyberspace," Center for Strategic and International Studies, May 22, 2013, http://csis.org/publication/private-retaliation-cyberspace.

77 "The International Code of Conduct for Private Security Service Providers," Swiss Federal Department of Foreign Affairs, October 8, 2010, http://www.state.gov/documents/organization/150711.pdf.

78 Convention on Cybercrime, Treaty No. 185, Council of Europe, November 23, 2011, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

79 The authors gratefully acknowledge the contribution of Scott Kannry to this section.

80 Jason Healey, "A Nonstate Strategy for Saving Cyberspace," Atlantic Council, January 2017, http://www.atlanticcouncil.org/images/publications/AC_StrategyPapers_No8_Saving_Cyberspace_WEB.pdf, 26.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

The **Carnegie Endowment for International Peace** is a unique global network of policy research centers in Russia, China, Europe, the Middle East, India, and the United States. Our mission, dating back more than a century, is to advance the cause of peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

The **Carnegie Cyber Policy Initiative** focuses on addressing international cyber policy challenges, as cyberspace is increasingly central to international security and diplomacy.

BEIJING BEIRUT BRUSSELS MOSCOW NEW DELHI WASHINGTON

THE GLOBAL THINK TANK

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org