CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

DECEMBER 2018

Governing Private Sector Self-Help in Cyberspace: Analogies From the Physical World

Wyatt Hoffman and Steven Nyikos

Governing Private Sector Self-Help in Cyberspace: Analogies From the Physical World

Wyatt Hoffman and Steven Nyikos

For your convenience, this document contains hyperlinked source notes indicated by this teal colored text.

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.

CONTENTS

Executive Summary

Cyberspace is transforming the relationship between states and private entities. States have benefited immensely from the autonomy given to corporations driving technological innovation, but rapid innovation and growing societal dependence upon data and information and communications technologies have brought significant exposure to cyber risks. The consequences of these risks increasingly extend beyond corporate assets to broader public safety, economic prosperity, and even national security interests. Yet despite growing awareness of the extent of the problem, the roles and responsibilities of government and the private sector in cyberspace remain largely ambiguous.

This ambiguity leaves unresolved the proper scope and limits of self-help in cyberspace: How far are private actors allowed, expected, or even obligated to go when providing for their own security from malicious cyber activities?

Increasingly frequent and costly cyber attacks targeting the private sector routinely surmount basic cybersecurity measures. To counter this threat, private actors globally are contemplating or engaging in risky activities, including hacking back into the computer networks of their attackers to punish them or disrupt their activities. The absence of clear international rules of the road for private actors in cyberspace threatens to create a serious gap in global governance enabling potentially destabilizing private sector activities. There is an urgent need to consider the emerging norms and desirable boundaries of self-help in cyberspace.

Unlocking the significant capacities of the private sector through a properly circumscribed self-help policy approach could offer an essential part of the solution to a deteriorating cybersecurity landscape. This is a growing strategic imperative for the United States and others struggling to manage the private sector's exposure to incessant cyber attacks by state and nonstate actors alike.

This study attempts to help navigate the risks and opportunities presented by private self-help in cyberspace. It aims to foster serious consideration of the realistic boundaries of self-help and its potential role in private sector cyber defense.

Self-help in cyberspace includes a wide range of activities, from basic measures securing assets (for example, firewalls and encryption) to more assertive defenses designed to thwart attacks and even retaliatory cyber operations against attackers' computer networks. The focus here is primarily on those activities that exceed the limits of purely passive defenses—activities that could be perceived as similar to the use of force in the physical world. Such activities are the subject of growing contention

and raise significant concerns, including risks of collateral damage to innocent third parties and the consequences of measures with transnational impacts.

The aim here is not to resolve the complex dilemmas for law and policy presented by these measures. Before such legal and policy debates can be resolved, more fundamental questions need to be addressed: What principles should define reasonable defensive behavior, and how should governance be approached in a transnational market of security services? This study outlines the contours of a pragmatic approach to answering these questions with a focus on minimizing risks and incentivizing responsible conduct.

Lessons From Historical Experience

Cyberspace presents novel complexities and dilemmas. But the challenges of governing private actors undertaking security roles are not unprecedented. Historically, there has always been a need to strike a balance between the roles of the state and private actors that places some burden of risk on the latter and allows for some extent of self-help. The emergence of unique roles and capacities of the private sector in cybersecurity is in many ways an extension of deeper trends in the physical world that characterize the currently shifting relationship between states and private actors.

This study draws from historical and contemporary experiences with various manifestations of self-help in the physical world analogous to cyber activities. It examines analogies from the U.S. domestic context and from international governance efforts. The examples range from electric fences and other measures individuals take to defend their property to the quasi-military activities found in the global industry of private security contractors.

Analogies have inherent limitations but offer useful heuristics for thinking through the dilemmas posed by self-help in cyberspace. They capture different facets of this challenge that blurs traditional distinctions—foreign and domestic, public and private. The analysis here focuses on both *where* and *how* self-help should be realistically circumscribed. The insights from these analogies include specific principles and distinctions for governing defensive activities, complementary mechanisms for managing risks and incentivizing behavior, and lessons from processes of governance in similarly complex, global domains of activity.

Directions for Policy

Creating space for legitimate and responsible self-help practices could begin to arrest negative trends in cybersecurity and reduce the pressure on governments to escalate their responses to cyber threats. Such space may even be necessary to forestall corporations' resort to riskier, destabilizing activities and vigilantism, or avert an equally undesirable trajectory toward an untenable situation for private sector cybersecurity.

Certain measures and practices clearly should be off the table for private actors. But within those constraints, there is significant space to explore a spectrum of defensive measures whose risks appear to be manageable and justified in some circumstances. Many of these defy traditional frameworks for forceful activities. They can be employed in ways tailored and proportional to threats, limited in impacts (for example, temporary or reversible), and conditional upon technical safeguards or certain defensive contexts.

This spectrum of cyber measures affords unique opportunities for self-help, but many such measures carry complex risks. They call for a nuanced approach to governing the behavior of private actors. Such an approach should examine, holistically, the incentive structure shaping private sector behavior, including competing and complementary forces such as regulation, liability, insurance, and market forces. Efforts to shape this incentive structure should be calibrated to the realistic limits of government control in this space and consider flexible, stopgap solutions. Finally, states' domestic approaches must correspond to the global nature of these activities. At a minimum, an attempt to foster a common understanding of rules of the road among like-minded states is needed. But the irresolution of fundamentally diverging views among states toward the legitimacy and legality of self-help activities should not impede practical measures to improve behavior.

This study attempts to define the broad contours of an approach to governing self-help in cyberspace by integrating insights from the analogies explored here. The result is four directions for policy:

- *Solidify absolute boundaries* of legitimate self-help to exclude those activities that would clearly be destabilizing internationally (that is, destructive hack backs). This calls for some convergence internationally upon norms that would build a firewall between legitimate self-defense and activities exclusively in the domain of state actors or oversight.
- *Raise the bar* for basic cybersecurity practices to limit the circumstances that would require more assertive defenses. If the vast majority of cyber attacks can be mitigated through basic cyber hygiene, then making more assertive measures conditional upon basic due diligence would immediately narrow the circumstances of their employment.

- *Clear the way* for self-help activities that would be broadly beneficial and relatively low risk, including a range of measures like digital beacons. Promoting more effective and less predictable defenses can create a broader deterrent effect that extends even to those not employing them.
- *Create the conditions to motivate responsible conduct* for those activities whose risks could be managed or mitigated. This includes a range of complementary approaches: leveraging key stakeholders in positions to shape norms and conduct (the insurance industry, financial sector, and so on), raising barriers to entry in the form of licensing or certification requirements, imposing liability for negative consequences, and creating incentives to guide behavior in a transnational market of security services.

Clear roles and responsibilities in cyberspace have yet to be negotiated. Yet de facto norms of self-help behavior are already emerging—driven largely by individual corporations' initiative and growing demands for aggressive cyber defense. Serious attention is needed to think through how to proactively shape the trajectory of this space of private sector activity. This requires moving beyond the false dichotomies that have dominated discussions (such as whether or not to allow hacking back). There are inevitable risks with any path forward regarding the role of the private sector. And in the current transient state of the domain, it is more important to identify feasible stopgap measures to manage these risks rather than attempt to define an ideal end-state. This study thus hopes to both help ground this debate in experience and stimulate further consideration of these questions.

Introduction

The cyber risk landscape has deteriorated in recent years. Massive ransomware attacks, large-scale data breaches, and discoveries of pervasive cyber vulnerabilities and aggressive, persistent intrusions into critical infrastructure and other sensitive targets all demonstrate an expansion and escalation of cyber threats. This trend appears likely to accelerate as sophisticated cyber capabilities proliferate further to globally dispersed malicious actors and the scope and scale of opportunities to launch attacks continue to expand. Meanwhile, the potential grows for systemic cyber risks to impact public safety, economic prosperity, and national security.

Far from protecting the private sector from cyber threats, many states are exacerbating the problem. Most governments are preoccupied with securing their own networks and critical infrastructure and lack the resources necessary to defend the private sector in any comprehensive manner. Many have strong aversions to assuming responsibility for private sector cyber risks. Even when they do seek to respond to and can attribute malicious activity, their responses are often impaired by concerns of escalation, retaliation, and other unintended consequences. Moreover, states remain largely focused on exploiting cyberspace—often for legitimate national and international security purposes. Yet offensive cyber capabilities deployed or accidentally leaked have been reverse engineered and redeployed by malicious actors, further undermining the private sector's security.

By exposing private entities to the malicious activities of foreign nation-state hackers, criminals, and terrorists, cyberspace has weakened the buffer that states traditionally provide between their citizens and external security threats. This is not to say that governments are doing nothing; many have assisted the private sector with cybersecurity.[1] But their efforts have largely been outpaced by the escalation of cyber threats that the private sector generally cannot rely on law enforcement to protect it from. Cyber threats thus pose a fundamental challenge to the state's role as the ultimate guarantor of its citizens' security.

Consequently, for private sector entities forced to navigate this deteriorating landscape, cybersecurity has become largely a matter of self-help—that is, protecting their assets without recourse to law enforcement.[2] At the most basic level, self-help in cyberspace includes common measures to secure oneself from malicious activity—an expectation of personal responsibility reflected in the frequent reference to cyber hygiene.[3]

But increasingly sophisticated and costly cyber attacks that surmount basic cyber defenses have motivated some private entities to engage in more assertive forms of self-help. This includes companies undertaking, contracting, or offering a spectrum of measures often referred to as active

cyber defense (ACD).[4] Some such measures are potentially beneficial not only for companies' defense but also for deterring cyber threats more broadly. Yet many entail significant risks, including potentially disrupting or damaging networks of innocent third parties (particularly if a cyber attack is misattributed).

There is a concerning lack of clear rules of the road for this growing, transnational space of private sector activity. Many states have laws criminalizing hacking that prohibit defensive measures that would intrude into attackers' or third parties' systems or networks, even for self-defense. But such laws often have significant ambiguities in application and unclear enforcement.[5] Policymakers globally are struggling to find effective formulas to govern this gray space of active defense.[6]

Inconsistencies among national approaches contribute to a fragmented regulatory environment internationally. The absence in many states of clear legal limits on such activities in cyberspace encourages aggressive practices that blur the line between defense and offense, such as hacking back into the networks of attackers.[7] Furthermore, offshore activities or contracting make it possible to circumvent the constraints that do exist. With a nascent transnational market for aggressive defensive and even offensive measures, a gap in governance is emerging globally that cannot be addressed by national regulatory approaches alone.

The scope of appropriate private sector self-help is ill-defined because there is little clarity regarding both minimal expectations for corporations to undertake basic cybersecurity and maximal limits on aggressive defenses. This results in corporations taking divergent strategies to manage their growing exposure to cyber risks. Some react with relative complacency, doing the minimal amount necessary to meet expectations or requirements. Others adopt a more aggressive defensive posture, resorting to self-help practices that come with their own set of risks.

These pressures on the private sector lead many companies to directly or inadvertently channel cyber risks—toward subcontractors, consumers and shareholders, governments, a nascent insurance market, or outward to attackers and potentially innocent third parties (through collateral damage). The burden of risk often falls to those with less ability to understand or manage it, sometimes without them even knowing—for example, innocent third parties. Even those companies that are proactive and effective at mitigating cyber risks may find it increasingly hard to do so in the face of escalating threats.

This state of affairs presents a precarious situation for policymakers. Attempting to shape private sector behavior in one area may have ripple effects by incentivizing companies to channel risks elsewhere. These effects can be difficult to anticipate, and cyber risks are often inscrutable even to

the companies themselves. Further, these risks and activities are not contained by national boundaries. Countries are trying to set domestic rules for activities that have transnational externalities. The lack of global norms creates the potential for a gap in governance of private sector behavior that could destabilize cyberspace in unprecedented ways. Policymakers are under increasing pressure to address cyber risk but lack an effective formula to balance these factors.

This study examines the emerging boundaries of private sector self-help in cyberspace to help navigate these policy challenges. It explores the role that self-help might play in combating malicious activity and contributing to order in a rapidly evolving domain that challenges traditional assumptions and approaches to security, with a focus on how to circumscribe and govern self-help. But the scope of this study is pragmatic, starting with an appreciation of the limits of law and regulation as well as the inevitable risk trade-offs, and concentrating on realistic approaches to motivating responsible behavior.

The approach here draws from historical experience. The process of fostering rules and norms of behavior is often iterative and can be difficult to navigate in an emerging domain of activity. When considering the desirable and realistic boundaries of self-help behavior, it is useful to reference examples from the physical world. This study examines a range of activities from the physical world analogous to specific cyber measures and the frameworks and mechanisms that evolved to govern these activities. Examples include the use of electric fences or mantraps to protect private property or the employment of private armed guards.

Self-help in cyberspace could take many forms, from basic measures to secure assets to retaliatory cyber operations against malicious actors. This study focuses primarily on those actions near, or in some cases transgress, the upper limits of defensive behavior—measures that appear similar to force in the physical world. These measures comprise much of the current ambiguous space and pose the most difficult dilemmas (in contrast to the more innocuous basic cybersecurity measures).

The diverse range of technical phenomena this entails cannot be captured by any single analogy. Thus the first half of this paper catalogues various frameworks for governing specific self-help activities in the physical world in the U.S. domestic context. The second half focuses on the governance of private self-help activities in the international context through various state-centric and multistakeholder approaches. The study concludes with an examination of the individual and collective insights from these analogies for governing self-help in cyberspace.

Each analogy demonstrates a dynamic balance struck between the legitimate interests of private actors to defend their property and the negative consequences of self-help behavior. How this

balance emerges and evolves can offer valuable insights: principles to govern forceful measures; lessons for weighing and balancing the competing equities at stake; mechanisms to incentivize and shape the behavior of private actors; and approaches to resolving the challenges of governance in a transnational domain of private activity. Individually, the analogies may vary in how readily their principles and precedents translate to the cyberspace context. For this reason, this study does not dwell on any single analogy but focuses on the collective insights from a broad survey of manifestations of self-help.

The objective of this study is not to resolve the complex legal, policy, and strategic dilemmas posed by these activities. More modestly, it seeks to provide useful heuristics for understanding and navigating these dilemmas by grounding them in historical experience. There is steadily growing pressure in the United States and elsewhere to revisit legal constraints on aggressive private sector cyber defenses.[8] Before the legal questions surrounding these activities can be answered, some fundamentals must be considered, including the principles that should govern this arena of private sector activity and how law and regulation play a role within the broader incentive structure shaping behavior. While any path forward regarding self-help needs to be reconciled with existing law, a discussion of whether and how to amend the Computer Fraud and Abuse Act in the United States or other relevant laws is beyond the immediate focus here.

This study, therefore, does not offer legal opinions on the applicability of existing law to actions in cyberspace. The examination of legal precedents from real-world activities is not to suggest that these precedents can or should necessarily apply as a legal defense for cyber activities. Rather, the focus is on how those precedents reflect an effective balance struck through similar dynamics as those at play in cyberspace, and their usefulness in thinking through cyber analogs. Any reference to possible liability or legality of a particular action in cyberspace is offered merely as a normative consideration rather than a legal opinion.

Self-Help in the Historical Context

Current debates over private entities' use of controversial defensive cyber measures tend to fixate on their technical and legal dimensions: What limits should be placed on technical measures employed by defenders? Should defenders be allowed to engage in unauthorized access for the purposes of self-defense? However, underlying these disagreements are more fundamental, unresolved questions: What constitutes force in cyberspace? Should the government maintain a monopoly over the

legitimate use of force in cyberspace—and is it even possible to do so? Placing these questions in the broader context of self-help draws attention to some of the assumptions that undergird these debates.

There is a temptation to view self-help, generally speaking, as antagonistic to state sovereignty and authority. This flows from a familiar narrative: the modern state evolved to supplant self-help as a guarantor of security; private actors agree to largely forego self-reliance for their defense. It follows that self-help in cyber could be atavistic—a return to a more primitive, lawless state of affairs. Indeed, debates over whether to allow more aggressive cyber defenses frequently invoke the Wild West as an admonition against ceding any ground to the private sector.[9] Allowing self-help is seen as an irresponsible retreat by the state from the cyber domain and a weakening of its sovereignty.

Yet this view rests largely upon a mischaracterization of the historical nature of self-help. There has always been a balance struck between state and private responsibility that has both placed some burden of risk on private actors and empowered them to undertake their own security within limits. This balance has varied across national and cultural contexts. It has also evolved in response to changing security circumstances and the efficacy of states' and international institutions' management of threats. But it does not exist simply along a continuum with the state on one end and the private sector on the other. Rita Abrahamsen and Michael Williams have argued that with globalization:

> State power is certainly reconfigured, but it is not necessarily weakened. Instead, the very distinctions between the public and the private, the global and the local are rearticulated and reworked, giving rise to new practices and forms of power that cannot be neatly contained within geographical boundaries of the nation-state.[10]

Rather than a linear trajectory toward the gradual elimination of self-help, these scholars argue that there has been a sustained trend since the end of the Cold War in developing and developed states alike toward the empowerment of the private sector in security functions—from technologies for surveillance and home security to private military contractors. This is in part a result of globalization and evolving technology creating risks that demand increasingly specialized, on-demand, and rapidly adaptable security services. Global business risks fueled the rapid growth of the security services industry, with specialized businesses offering comprehensive security and risk management services tailored to multinational corporations.

Often it is commercial activity that generates demands for risk management that are not easily met by states, as they are focused on traditional policing functions and typically resistant to assuming

responsibility for private activities. The business risks of multinational corporations, which often divert profits away from states and blur distinctions of nationality, are even less politically legitimate for governments to assume responsibility for.

In this light, the emergence of self-help in cyberspace appears less of a novel phenomenon than an extension of a sustained trend in the physical world: transnational commercial activities driven by evolving technology and a global operating environment are generating new risks that exceed the capacity or willingness of governments to assume responsibility for. Companies and private individuals are largely left—and in many cases encouraged—to secure themselves. As in the physical world, growing awareness of risk in cyberspace is contributing to a rapidly expanding market for managed cybersecurity services and the outsourcing of more aggressive self-help services. The cybersecurity industry appears to be on the same trajectory toward globally operable, integrated security solutions that have characterized private security in the physical world.[11] States contribute to the demand as they often turn to private companies for both defensive and offensive capabilities and services.

Self-help in cyberspace, therefore, should not be viewed inherently as an aberration even as it presents unique considerations. Central to the new economic and security environment is the fact that the private information and communications technology (ICT) industry constructs and maintains much of the physical and logical infrastructure that comprises cyberspace. Malicious actors are constantly operating within and through private sector assets. As Lucas Kello put it: "In the past, the enemy's presence in essential domestic terrains signaled the failure of security policy; today it is a starting axiom."[12] Consequently, companies making routine decisions in the development, production, and distribution of ICTs and their incorporation into other products are simultaneously shaping the range of possibilities for cyber operations, whether or not there is awareness or weighing of these security implications. In some cases, these decisions can have systemic impacts, given the interdependence of ICTs and widespread reliance on common platforms and services. Questions surrounding the scope and limits of private sector self-help should thus be viewed in the context of the private sector's central role in this environment.

The ability of the private sector to directly and inevitably shape the risk landscape contributes to a core policy dilemma. If states attempt to preclude self-help and undertake responsibility for the security and defense of the private sector, they may create a moral hazard; companies will feel less inhibition to take actions that expand cyber risk since the responsibility and costs for managing it will fall to the state. Yet an overly permissive environment for self-help potentially encourages companies to channel risk toward third parties by engaging in aggressive defensive (or offensive) activities that may have collateral damage. The fact that these risks transcend national boundaries

adds an additional level of complexity because they may incentivize jurisdiction shopping, offshore contracting for services, and the like.

This dilemma is only beginning to emerge on a global scale. But as basic, passive cyber defenses become increasingly insufficient to contend with sophisticated threats, the dilemma seems destined to become more pronounced. Of course, this is not to suggest that private actors should disregard basic cybersecurity practices, which can mitigate the vast majority of malicious activity. Rather, the current trajectory suggests that reliance upon passive defenses alone will become untenable. This may necessitate a balance between public and private roles that allows for effective self-help while incentivizing responsible behavior in this unique environment.

It is essential to consider the full range of forces that interact to shape this balance. As in the physical world, norms and practices for cyber activities are not simply technologically or statutorily determined but are the outcome of multiple, competing influences on the private sector including expectations of corporations' responsibility for their security and the demand for and supply of security services globally. A fixation on the de jure distinctions between public and private responsibilities risks overlooking the de facto distinctions that emerge over time. The question is never as simple as whether to allow or prohibit a given self-help practice. States have a range of tools at their disposal to either counteract the forces giving rise to behavior they view negatively or induce behavior they view positively. As a prelude to the specific analogies, it is useful to sketch out this full spectrum of policy approaches toward self-help practices:

Figure 1: Spectrum of Government Policies Toward Private Sector Self-Help

States may take a variety of approaches, with varying levels of intervention, to restrict engagement in self-help practices they view negatively:

- *Prohibit*—The state both formally prohibits an activity and actively undertakes to monopolize its practice, whether by punishing private actors for engaging in the activity or simply by exercising control over the capabilities necessary to do so.

- *Tolerate*—The state expresses formal disapproval of an activity while falling short of directly intervening to prevent its practice. It may create barriers to entry or other constraints to limit engagement, such as through licensing requirements. Or it may take a more passive approach, creating disincentives, such as leveraging market pressures to shape behavior.

States similarly intervene to various degrees to support and bring about certain self-help practices they view favorably:

- *Encourage*—The state demonstrates its approval of certain activities but largely leaves it to other forces, such as market pressures, to induce them. It may remove barriers to action or create incentives to nudge private actors to undertake an activity. More assertively, it may actively facilitate certain practices and empower private actors by providing legal authorization, building private sector capacities through training or public-private partnerships, or offering other forms of assistance.

- *Require*—The state mandates an activity and may even punish actors for failing to undertake it. This may occur for entities whose failure to exercise basic self-help could be broadly detrimental to the public (for example, the security of nuclear facilities).

This spectrum is useful for underscoring several distinctions relevant to a policy approach to any form of self-help: tacit versus explicit positions and rules; direct regulation versus indirect influence; nominal policy versus action to realize some desired outcome; among others. At the extreme ends are the most assertive forms of governmental action, while in between is a continuum of approaches. The categories represent mere demarcations along this spectrum rather than discrete points. In reality, a state's position may be ambivalent or even incoherent and difficult to place in any one category. It may have contradictory policies if different actors or agencies within the government push in different directions. Moreover, its approach may shift over time, with formal changes in policy lagging behind changes in practice. The government may simply remain ambiguous toward an area of activity, or leave it to be addressed by publicly initiated civil litigation.

It is reasonable to expect that for the foreseeable future self-help will play a relatively significant role in cybersecurity. Cyber threats are incessant and constantly evolving. The speed of cyber attacks in

many cases vastly outpaces law enforcement action. Corporations' cybersecurity needs are even more esoteric, specialized, and concentrated in private sector expertise than the physical security needs that have fueled the private security industry. Moreover, the private sector faces business risks that defy the application of traditional distinctions such as geographic location or legal jurisdiction. These risks can vary widely across industries or even among individual companies in the same industry. There is a growing recognition that these factors necessitate a high baseline level of constant risk management, including preparation for, resilience against, and recovery from attacks, rather than achieving some steady state of security—whether provided by the state or otherwise.

At the same time, the need to circumscribe self-help is ever greater in cyberspace, where individual corporations have capabilities that rival (or even exceed) some nation-states. A single company's defensive action could spark an international incident or result in significant collateral damage that spills across national boundaries.

These observations serve as the starting point for the following survey of analogies that examines where and how various forms of self-help have been circumscribed historically, and what this suggests for navigating the questions posed by emerging and evolving forms of self-help. Insofar as past experiences with self-help in a variety of forms have been shaped by the same dynamics currently at play in cyber, these experiences can provide important and useful insights and a foundation for defining the rough contours of a framework for governing self-help in cyberspace.

Self-Help Frameworks in the United States

The U.S. domestic context demonstrates the extent to which private actors undertake the protection of their assets in the physical world and how boundaries emerge and evolve to govern such activities. These boundaries are often formed by complementary incentives and mechanisms shaping behavior. The government sets absolute limits through criminal liability, ruling out activities deemed illegitimate for private actors due to their disproportionate impacts on third parties or even attackers. Within these limits, the space of reasonable and legitimate conduct is often defined by civil liability—the potential to be sued for monetary damages resulting from harmful effects of self-help.

Civil liability plays a key role in balancing the competing equities at stake with self-help—the legitimate interests of the defender and the risk of harm to third parties. The discussion here thus focuses heavily on the role of civil liability in circumscribing self-help activities that pose risks to third parties, frequently in combination with formal and informal regulatory mechanisms.

Historically, the evolution of domestic civil liability has followed a consistent path. First, certain actions are deemed unacceptably destabilizing or harmful to society, typically due to a successful lawsuit on behalf of an injured party. Then, the resolution of that lawsuit adds to an ever-growing body of civil law that draws boundaries for acceptable behavior.

Such a body of law is now gradually accumulating to address self-help actions in cyberspace. Through both successful and failed lawsuits, the expectations and limitations across a range of self-help behaviors are being loosely outlined. However, for many cyber measures, there is a lack of both jurisprudence and practical experience with their use and consequences. This makes it difficult to try and proactively address the legal ambiguities that exist. Referencing historical examples of self-help in the physical world is useful when considering the potential boundaries of self-help activities in cyberspace.

This section begins by exploring a range of activities in the physical world analogous to specific defensive activities in cyberspace. Here it is useful to distinguish those forms of self-help analogous to preemptive or preventive acts outside of a home network prior to an intrusion from those closer to mitigation and retaliatory action during and after an intrusion. After laying out this spectrum of activities, this section then examines different frameworks for selectively authorizing self-help activities or actors.

Detection, Preemption, and Prevention Outside the Home Network

Public Surveillance: Security Cameras

Security cameras or perimeter sensors to detect criminal behavior in the physical world are analogous to detection capabilities outside of a defender's network in cyberspace. Typically, security cameras record an individual's property but may also cover public spaces like a sidewalk or street. Under U.S. law, cameras can record activities anywhere there is not a reasonable expectation of privacy on behalf of the individuals being recorded.[13] This guideline is court-determined based on a variety of factors. Generally, spaces that are open for community use do not have such an expectation.[14]

Security cameras demonstrate a compromise between competing equities of privacy and security, allowing for activities of limited intrusiveness for the benefit of combating crime. Applying this principle to cyberspace, defensive measures outside of a home network whose impacts are limited to information gathering could be justified, provided their information gathering was confined to areas where there is no reasonable expectation of privacy. When considering what such a compromise

might look like in practice, it is pertinent to reflect on how these precedents have extended from the physical space to other domains—namely communication technologies.

The widespread adoption of telephone technology created similar tensions between competing equities for privacy and security. In 1928, shortly after the invention and rapid spread of telephone technology, the Supreme Court case *Olmstead v. United States* determined that a wiretap did not violate an individual's Fourth Amendment right against unwarranted search or seizure, as it did not constitute a search of premises.[15] This was overturned in 1969 by *Katz v. United States*, which famously stated that the Fourth Amendment protects people, not places.[16] Thus, despite not constituting a physical search of premises, wiretapping requires a warrant because it is a search of an individual's communications. This new perspective hinged on individual rights—specifically that of privacy—and established that Fourth Amendment protection applies when an individual has a reasonable expectation of privacy. This is not limited simply to physical space, but extends also to a person's communications or activities (including online). The expectation of privacy requirement has since expanded to apply to both federal and private intrusions into an individual's sphere of activities via a multitude of technologies, including security cameras and cyberspace activities.[17]

Precisely where and how privacy rights extend to cyberspace is a subject for a much broader discussion. But there is a need to strike a balance between privacy and security as in other domains. A reasonable expectation of privacy has already been extended to protect the explicit content of communications in cyberspace under U.S. law.[18] However, it does not appear to extend to certain types of data like bandwidth usage or data from internet service providers (ISPs), or even individual traffic data.[19] Thus, when considering the legitimacy of measures that collect such kinds of data, it is important to weigh their limited impacts on privacy against their contribution to security.

This framework is potentially relevant to a range of measures and network monitoring activities that raise potential privacy concerns.[20] "Traceroutes" or "tracebacks" used to track potentially dangerous traffic provide an illustrative example. Traceroutes are a tool to track packets sent along an internet protocol (IP) network, originating from the home network that employs the traceroute. Meanwhile, tracebacks are an attempt to properly attribute the source and path of incoming packets.[21] Often, traceback methods rely on packets being marked by public routers as they pass through the internet, in a manner similar to public observation by security cameras, or tracking by private investigators (who also do not have legal access to information where owners have a reasonable expectation of privacy).[22] Thus, traceroute and traceback techniques do not typically incur civil liability. However, if tracking were to become overly intrusive, and reach into areas where citizens are ruled to have a reasonable expectation of privacy, such as the content of their communications, the result would likely be some form of injunction against such behavior, as well as either a fine or monetary

settlement. In keeping with the development over time of the reasonable expectation of privacy standard, the dispositive factor in whether intrusive activity may incur liability is whether that activity exposes private information of the individual, not necessarily the methodology used to get such information.

The challenge of balancing privacy and security in cyberspace is complicated in part because the appropriate level of privacy protection in this landscape remains a moving target. The salience of particular kinds of digital information to privacy rights is still unsettled. However, situational awareness and intelligence gathering in the environment outside of home networks appear to be increasingly necessary for effective defense against sophisticated cyber attacks. While it is important to draw lines to protect privacy, it may be necessary to create space for such measures provided their impacts fall below a certain level of intrusiveness.

Dangerous Perimeters: Electric Fences

Electric fences on property borders use force against intruders, which inevitably carries some risk of harmful impacts to innocent parties that come in contact with them. U.S. laws governing electric fence placement and voltage operate on a state-by-state basis, but there is a national prohibition against mantraps that use deadly force. [23] According to U.S. law, reasonable force is permitted to protect against the theft of property if the force reasonably appears to be necessary to prevent or terminate an intrusion into, or interference with, an individual's property—and doesn't violate any other explicit law (like damaging a neighbor's property).[24] However, automated deadly force in the defense of property is never acceptable. Thus, a fence with enough voltage to kill someone is illegal, while a stun fence (or barbed wire) is not.

This distinction arises from a focus upon human life and safety over the value of any property when determining legally acceptable uses of force. The prohibition against mantraps that use deadly force was famously exemplified in *Katko v. Briney*,[25] in 1971, when the court explicitly stated, "The law has always placed a higher value upon human safety than upon mere rights in property" and justified a thief successfully suing their would-be victim for booby-trapping his barn with a tripwire shotgun.

By extension of this logic, in the cyberspace context, if a network intrusion or data theft is initiated, then automated reasonable force could be used to counter such a threat. Importantly, any actions that result in bodily harm, death to individuals, or damage to a third party's property may not be reasonable and can create liability for the entity engaging in these techniques—just as traditional booby traps would.

The limits of acceptable forceful perimeter defenses in the physical world are a function of their impacts, not just their location. This presents a complication for thinking through what an electric fence in cyberspace looks like. IP blocking is a common technique used for network defense at the enterprise level. The technique filters and blocks connections and packets from specific source IP addresses (where packets are sent from), or a range of IP addresses that are considered malicious.[26] However, this is more analogous to a fence or gateway that is not electrified or dangerous.

Alternatively, a network may employ techniques to deflect traffic, treating incoming packets based on their source IP address and presumed threat level.[27] If that network then automatically responds to certain IP ranges with aggressive action external to the network (like responding with packets that freeze or damage systems—logic bombs—directed at the purported source IP addresses), liability can result if people are harmed when those systems fail, or if the source IP address is misattributed and third party systems are impacted. Yet more limited, temporary, or reversible disruptions of an attack infrastructure could arguably constitute a reasonable response, even though the impacts would technically be outside of the defender's network perimeter.

Precedents from the physical world need to be adapted to the unique geography of cyberspace. The location of an effect should not be the *only* consideration in defining a reasonable response to a cyber attack. The scope, scale, and severity of impacts from the defensive measure should be weighed against the offensive threat. Causality is a key factor in determining liability for self-help techniques that are in any way tied to bodily harm or death. Specifically, the automated technique must be both the cause in fact and the proximate cause of an injury.[28] If an automated measure misattributes the source of an intrusion, and launches a logic bomb that takes down an external server as a response, would a court find any resulting physical harm to an individual had been a reasonably foreseeable result? What if the measure impeded hospital or critical infrastructure server function? Ultimately, by enacting aggressive self-help measures that reach outside their home network, a defender risks harming individuals. Given the higher value that U.S. law places upon human safety over rights to property, as exemplified in *Katko v. Briney*, courts may be likely to hold the defender responsible for the harm in such cases.

In the case of automated, indiscriminate measures with potential collateral damage, strict limits to prevent physical harm are necessary. But the same physical world precedent suggests it is worth exploring how to define the technical and circumstantial parameters that would define a reasonable, justified defensive response subject to the same principles as forceful activities in the physical world.

Mitigating and Retaliatory Actions

Castle Doctrine and Stand Your Ground Laws

In many jurisdictions, an individual has a legal duty to retreat in the face of violence before using self-defense. However, the Castle Doctrine is a legal framework (adopted on a state-by-state basis) whereby an individual in their home has no such duty, and can immediately use force in self-defense (often up to and including deadly force). This, however, is exclusively for self-defense of a person (not of property), and, moreover, a corporation's headquarters (or servers) do not qualify as a legal "dwelling." As a result, this has very limited applicability in the cyberspace context. This would be confined to extreme cases where there is a reasonable expectation that failure to arrest the cyber attack could ultimately result in physical harm directly or perhaps indirectly, such as by endangering the performance of a life support or an essential ventilation system. Similarly, defensive action to disrupt an attacker might seem justified to prevent an attempt to spoof some instrumentation to provide a false reading that could, in turn, result in misguided and life-threatening corrective action and/or cause panic (for example, by tinkering with the vital control systems of an operating nuclear power plant).

Similarly, multiple states have Stand Your Ground (SYG) laws, which abolish an individual's duty to retreat before using self-defense. While the specifics vary from state to state, all such laws require that the individual standing their ground must be faced with some level of physical threat to their person (not to their property). Often, confusion arises because SYG laws apply to robbery attempts (which is theft via threat or use of force) but not to larceny or theft (which is simply theft without any implied danger to a person's safety). Stand Your Ground laws are exclusively for the self-defense of a person, and are rooted in legal protections of human life as opposed to property.

The jurisprudential prioritization of human safety over property remains relevant to self-help in cyberspace: in cases where a private entity's data or services are crucial to human safety, the imperative of defending their integrity and availability may justify measures that risk disruption or even, in extreme cases, damage to the networks of third parties. However, these two frameworks are mentioned here primarily to address their inclusion in conversations regarding self-help in cyberspace. Neither are properly applied to the protection of property, and thus their insights are limited to specific scenarios of threats to human safety, as described above.

Booby Traps

As noted previously, mantraps that use deadly force are not an acceptable means of protecting property. Booby traps that use exclusively nonlethal force, however, are potentially defensible. Automated pepper spray, deterrent alarms, and similar systems may fall under the category of reasonable force in defense of property if they do not cause excessive injury to persons, but rather deter and/or track intruders. This includes passive measures like internal security cameras that document the behavior of intruders. However, any automated defense cannot exceed what would be legally permissible in person if a threat to property (but not to life) existed.[29] Additionally, if nonlethal booby traps result in grievous harm (even to an intruder), or ensnare someone with a right to be on the property, such as a police officer with a warrant, then civil and potentially criminal liability could result.

In the cyberspace context, setting virtual and automated booby traps for network intruders, including methods of tracking their intrusion, only exposes a company to liability if any form of physical harm comes to the intruder, third parties, or third party property, or if retributive measures reach externally into private networks as a response. This is an instance in which the legal focus on bodily integrity, and lack of corporeal presence in cyberspace, works in favor of the defending network. By logical extension, it seems reasonable to put in place an extensive home network of cyber booby traps as long as they do not have impacts outside of the network borders (as compared with physical booby traps, which must be very limited in capacity).

Two methods of setting cyber traps in a home network are called honeypots and tarpits.[30] Honeypots are decoy systems that appear attractive to intruders, and have mechanisms that log the attackers' behavior once they are inside to gain information about their tactics and motivations.[31] A similar practice on a smaller scale is called a honey token. Attractive, but false, information is created as a lure for intruders. In a perfectly secure system, nobody should interact with that data. If someone does, then they can be identified and their motivations potentially exposed.[32] Often, a padded cell approach is used to trap intruders into a honeypot system by indicating that their intrusion has been successful, supplying false data, and notifying administrators of the intrusion details while the intruder remains within the fake system. This is analogous to a silent alarm alerting the police while an intruder remains inside the premises. Tarpits are a tool commonly used to address direct denial of service (DDoS) attacks.[33] Tarpitting identifies incoming malicious traffic (typically based on attributed source IP address) and slows it to the greatest extent possible, to disincentivize attackers from connecting to the network and limit the potential for a DDoS attack to overwhelm a network or server. Both honeypotting and tarpitting use no force against the attacker, and are entirely within the home network, so would not likely be subject to liability.

The most salient takeaway from this analogy is that any self-help actions within an enterprise network's borders are acceptable, so long as no physical harm results. But here again the geography of cyberspace impedes the straightforward application of precedents from the physical world. It may be possible in some cases for defenders to set traps in their networks that combine measures like honeypots with code that could be used to gather information from attackers' systems or even disrupt or damage them.

In extreme cases where aggressive external action is taken based on the information gleaned from honeypotting, such as malware implantation on adversarial networks, civil and potentially even criminal liability is highly likely to result. This constitutes a hack-back and is illegal. Such an act would be analogous to deterring an intruder with nonlethal booby traps, following them home, and intruding into their dwelling and setting fire to it as a response. However, implementing a narrowly tailored defensive measure activated by the intruder with limited impacts to disrupt attack infrastructure might be more akin to slashing the tires of a getaway car. At its core, this is a question of whether and how the use of a computer or network for malicious purposes should affect the owner's rights against intrusion or disruption. This question will be explored further in other examples below.

Citizen's Arrest

To stop a perpetrator before or during a felony, a private citizen has the right to use the level of force that is reasonable and necessary to detain an individual in preparation for law enforcement.[34] It is stressed in this framework that the force used is reasonable and necessary. Further, the detention is solely for the purpose of preparing for law enforcement (at least in theory). In practice, this framework has a very permissive interpretation—in South Carolina, shooting a fleeing suspect of a felony has been ruled to be reasonable and necessary force for the suspect's arrest. [35]

The common law practice of citizen's arrest has historical roots as far back as English common law, when sheriffs encouraged regular citizens to apprehend would-be criminals even if law enforcement was not present. This practice continued in the United States without an official statutory description for some time, until it was codified on a state-by-state basis. Every state has roughly similar interpretations—there must be a reasonable belief that the apprehended individual has committed a crime, and the use of force must not be deadly unless there is a corresponding threat of injury or death, or, in some states, if the suspect committed a violent crime.[36]

Translated to cyberspace, if a cybersecurity company (as a private actor) has identified live threat activity on its corporate network, that company may identify and attempt to ensure the network intruder is detained within the network when they reasonably believe the attacker is in the process of stealing intellectual property. Detention may encompass temporary incapacitation or even reasonable damage to systems or computers involved in the attack so long as that damage is necessary to stop the ongoing theft and is in preparation for the involvement of law enforcement. Ostensibly, if such disruption or damage is limited to what is reasonable and necessary, its impact would be reversible and temporary (as opposed to permanently disabling). However, given the wide latitude of interpretation in physical citizen's arrest cases, such a limitation may not be practically enforced.

It is vital to differentiate this method of detention of attacking systems from the hack-back scenario, based solely on the fact that data theft is in-process and must be stopped immediately. Such imminent theft may create an implied license to act with reasonable force based on the citizen's arrest jurisprudence. Interestingly, if the theft of the data in question has any implication of physical harm to others (or if the theft involved such harm in any way), an even greater license of aggressive action may be warranted. This is based on an extrapolation of the citizen's arrest allowance for deadly force in physical circumstances where the suspect committed a violent felony. At any rate, the potential damage of the cyber attack should serve as a differentiating factor for justifying certain defensive measures that risk harm to third parties.

Reasonable force may not be an effective means of halting an ongoing cyberspace intrusion or attack. One common tactic used to repel intrusions and ongoing thefts is called session disruption.[37] This simply severs the network connection that is facilitating a theft; it is a measure internal to a network that does not use force and can fairly be considered highly reasonable. However, this does not stop the attacker from switching IP addresses, attacking again (almost instantaneously), and continuing with an already partially completed data theft. So, while this may be a reasonably harmless defensive measure, it may not be effective enough to be meaningful.

In the physical world, it might be considered reasonable for a citizen to slash the tires of a getaway car if it was being used in the commission of a felony—harming property but not causing injury or death. Is it, by proxy, reasonable to impact or freeze an attacker's server, network, or access terminal? What if the attacker is stealing information that could harm people, or conducting the theft in a manner dangerous to third parties?

One recently developed active defense technique is known as poisoning the RAT (remote access tool). This method identifies a malicious intrusion, traces it back to its source, and uses security flaws in the ongoing connection between the source and the intrusion to penetrate the attacker's home

system, gather data, and affect damage.[38] Again, this approach is temporally limited—it can only be applied if a data theft is verifiably in-process, not after it has completed. Ascertaining risk to other services or tenants on a machine that is owned by a third party, where the attack has emanated from, is also important to consider. The application of a citizen's arrest paradigm to cyberspace has less settled jurisprudence than any other rationale discussed in this paper, especially since poisoning the RAT is a fairly new technique. However, given the extent of force that has been labeled reasonable in felony citizen arrest cases, it is potentially an acceptable and appealing virtual practice.

Fresh Pursuit

Hot pursuit, also known as fresh pursuit,[39] is an exception to laws against trespass or Fourth Amendment search and seizure protections. If a police officer is in immediate pursuit of an individual who has committed a misdemeanor or felony (or they reasonably believe that the suspect has), then they can follow that individual outside of their jurisdiction, or into private dwelling(s), and commit searches without a warrant. This exception may also apply to private parties, similar to citizen's arrest, and could permit the use of reasonable force to retake stolen property while in immediate pursuit of a thief.[40]

Fresh pursuit developed as a method of addressing crimes in which the suspect crossed jurisdictional boundaries—ensuring that the officers in initial pursuit would still be able to follow through with their arrest. It is very important to note but nonetheless unsurprising that the trespass exception for private parties has not developed as clearly as for police officers. Actions by private individuals that constitute a trespass are only speculatively protected by this common law framework. Thus, a private party risks criminal or civil liability by pursuing a fleeing thief onto private property.

After a cyberspace theft, retrieval of data may be able to proceed following the fresh pursuit framework. This speculatively allows private actors to identify, pursue, and use reasonable force against individuals/systems they reasonably believe to have committed a crime, in order to reclaim or at least disable their stolen property. The practical methods for doing so in cyberspace are limited, but hypothetically a client could track the data theft across public servers, or ask public server and router administrators to freeze or corrupt the data transfer before it reaches its home network.

If the stolen data has already been stored in a private location, then immediacy could warrant intrusion of a private network based upon a reasonable suspicion that stolen data resides therein. However, if this is an intrusion into the wrong network (due to a misattribution of IP) or unnecessarily damages the network while intruding, the private actor in pursuit risks civil and

criminal liability. It is therefore necessary to obtain both sufficient verification that the stolen data is there, as well as authorization of some kind to retrieve it. Such authorization can be either contractual or based on government authority, as will be discussed. But perhaps techniques that merely corrupt or otherwise deny unauthorized use of this stolen data without causing collateral damage should be considered a legitimate interpretation of fresh pursuit. In any event, there is a very fine line between ongoing data theft that potentially authorizes techniques like poisoning the RAT and taking aggressive action when the theft and ensuing flight is already complete, after which the legitimacy of taking the law into one's hands is increasingly questionable. This distinction is highly important in domestic U.S. law.

Of course, pursuit of an attacker outside of the defender's network might entail reaching across international boundaries and violating the domestic laws of another state. The acceptability of fresh pursuit across international borders in the physical world is limited by nation-to-nation agreements concerning the operation of foreign forces on sovereign territory. If the stolen data is stored in an area of questionable international jurisdiction, then any government authority should be either cooperative between nations or unilateral to support cross-border intrusions. Similarly, any contractual authority must be valid in the country where the network intrusion would take place.

Car Anti-Theft Devices

There are many devices that act as tracking systems,[41] and clients can legally install them on their car to automatically report the vehicle's location and allow law enforcement to retrieve it if stolen.[42] Importantly, these systems report the location of a car if it has entered onto private property, and can even disable the engine starter. Only the starter can be remotely disabled, not a running engine. This is because disabling an engine on a highway may result in serious accidents and loss of life (along with a high likelihood of civil liability for damages, or criminal liability for recklessness or negligence).

A historical, low-tech understanding of the legal principles involved in this analogy can be derived from the probable cause standard and exigent circumstances exemptions to the Fourth Amendment. If a police officer has probable cause to believe that illegal activity is taking place within a private residence (like hearing a scream from outside), they can present that probable cause to a judge and retrieve a warrant to search the premises in short order. However, if the need is immediate, that officer can prevail upon exigent circumstances to avoid the warrant requirement. Exigent circumstances are "circumstances that would cause a reasonable person to believe that entry (or other relevant prompt action) was necessary to prevent physical harm . . . the destruction of relevant

evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts."[43] A scream would certainly qualify. Arguably, knowledge that the car is on private property would qualify as well, given that it might be dismantled.

If intellectual property is stolen from a network and stored on a private server, it is important to certify that the data in question is in a specific location with some degree of certainty before using any authority to retrieve it. In the cyberspace context, beacon files can be created that, when opened, will ping the home network from whatever IP address they are stored, including private networks.[44] This effectively locates stolen files and may identify a thief. The resulting locational data may be used to either retroactively justify private actions (like intrusion into a network during fresh pursuit), or to inform policing authorities that then retrieve the data. Immediate police action may be justified under the exigent circumstances framework, given that data may be copied and sold extremely quickly. If sensitive information is stolen, an automatically encrypting, scrambling, or deleting mechanism could also serve as protection that is similar to disabling a car starter—rendering the stolen goods useless. An example of this in practice is that of white-hat ransomware that encrypts stolen files on the attacker's (or a third party's) system. [45]

While these actions technically involve the manipulation of data on a separate private network, they do not necessarily entail active manipulation by the defender and could follow the same legal framework as physical anti-theft systems. Importantly, just as only the engine's starter can be remotely disabled, if these mechanisms have any sort of automated virus or harmful effects to third parties (not necessarily the thief's network), it is possible for liability to result. Similar to the previous discussion of electric fences, the prioritization of human safety suggests both that careful limits should be placed on measures to ensure they do not pose significant risks to humans. Such measures, however, may be justified by the need to defend data critical to human safety.

Credit Card Fraud and Dye Packs

If credit card information is stolen and a fraudulent transaction takes place, it is common for the card issuer to block additional purchases immediately, or even cancel transactions that are already being processed based on the suspicion of fraud. This is done on a remote basis, sometimes without the direction of the actual card holder, under the auspices of account security (occasionally, it is even done improperly). This practice began as a response to rampant credit card fraud and expensive losses for both individuals and creditors—in 2014, global card fraud losses reached $16.31 billion.[46] Unfortunately, since it costs more to involve manpower, police, or investigation of the fraud, it is commonplace for issuers to simply write off the loss, cancel the card, and notify the owner.

Similarly, banks commonly insert dye packs into their money for use during robberies. These dye packs are meant to explode, leaving red dye on both the thief and the money, marking it as stolen and unusable. They may also release tear gas and/or ignite their surroundings, burning exceptionally hot, to make the thief drop their stolen goods.[47] It is important to note that these measures would incur liability if the thief faced grievous harm as a result (being blinded or excessively burned). Again, this is exemplary of a greater focus upon human life than protection of property.

The commonality between each of these analogies is the disabling of, or rendering useless, a stolen asset. A strategy could be employed that renders stolen data useless in a manner similar to credit card deactivation or dye packs, by corrupting or marking the stolen data. This corruption could be facilitated in one of two ways: either by actively reaching into private networks where the stolen data is stored (which would require some measure of authorization or immediate urgency, and would face complications in cross-border virtual thefts, as discussed) or through an automatic mechanism in the data itself that responds to unauthorized extraction from the home network (like an exploding dye pack)—a practice that would neither require knowledge of where the data is going nor authorization to implement (as it is an activity taking place on the home network, albeit the border). This is similar to the disabled starter analogy previously discussed.

Again, there is potential for embedding viruses or malware in the data file itself, to be triggered automatically upon its theft. White-hat ransomware exfiltrated from a defender's network could lock down an attacker's computer and require the user to contact law enforcement to regain access. If this were to harm third party systems or individuals or cause excessive damage to the individuals committing the theft, liability would result. However, if there were limited impacts contained to the thieving party's systems and networks then there exists some potential for this measure to proactively and aggressively safeguard intellectual property.

Government and Private Sector Authorization Structures

Across the spectrum of defensive measures discussed above, there are numerous ones that could be extremely useful in combating malicious activity but carry significant risks due to their potential impacts on external networks that, in many circumstances, would offset their benefits. Opening up these measures for engagement by any private actor could be extremely risky. However, there may be specific circumstances in which they could be undertaken responsibly as a legitimate response to malicious activity. It is worth exploring, then, how to create and define space for these measures without opening the floodgates.

There are alternative and complementary approaches to minimizing the risks of those self-help measures that are on the table. The analogies above have focused on the technical and circumstantial parameters of the defensive activities themselves as the primary constraints. It is equally important to consider approaches and mechanisms to limit the range of actors able to engage in defensive activities and the degree of autonomy and operational discretion given to those actors.

This section thus examines the legal frameworks and incentive structures within which private actors undertake roles complementary to government actors, or with some level of government authority, yet often without government immunity. In such circumstances, private actors expose themselves to physical and legal risk by undertaking these roles as contractors or subcontractors. This gives rise to demand for liability insurance to limit their exposure, which is provided subject to some conditions and exceptions that comprise a form of soft regulation. Examining these frameworks of authorization and liability guidelines is highly relevant for a cybersecurity industry in which the limits of private action and government involvement are yet to be determined, and both civil and criminal liability could result from conscious choices, as well as unintentional missteps.

Bounty Hunters

A bounty hunter is a private party that contracts to apprehend fugitives who posted bail but failed to appear in court. In the Wild West, bounty hunters were hired by local authorities to apprehend fugitives when the latter did not possess enough resources to find or pursue wrongdoers over hundreds of miles of open terrain.[48] This practice was first formally authorized in the United States in 1872, when the Supreme Court ruled that bounty hunters could act as the authorized agents of bail bondsmen, and gave them wide latitude.[49] The actions of a bounty hunter are empowered primarily by the contract that the fugitive signed to secure bail, which includes forfeiture of rights against intrusion or uses of force (this is why bounty hunters often face fewer restrictions than police officers in their actions).

Bounty hunting is regulated at the state level or below. Few states ban the practice entirely, while others allow it but do not permit bounty hunters to apprehend the fugitive (thus confining their role to simply tracking them down and notifying authorities). In eighteen states, bounty hunting is subject to almost no regulation.[50] Bounty hunters face less strict constitutional guidelines than police: they can break and enter into a fugitive's house without a warrant, seize the fugitive, use whatever force is necessary to obtain custody, imprison them, transport them across state lines, and act without new warrants. Coerced statements to a bounty hunter are even admissible in court.[51] To

be licensed, only four jurisdictions require taking a state exam, while a little more than one-third require formal training.[52]

With such permissive regulation, it is common for bounty hunters to receive civil lawsuits. The professional liability policy of the Professional Bail Agents of the United States is an example of bounty hunter insurance. It includes coverage for claims of assault, battery, false imprisonment, wrongful entry, and defamation.[53] These correspond with the expanded mandate of bounty hunters vis-à-vis law enforcement. Insurance companies can mitigate the risks of bounty hunters' activities by placing additional requirements on their coverage. The professional liability policy, for example, refuses to cover any claim arising out of the use of a firearm.

The key to this analogy is the legal mechanism for authorizing private activity that would otherwise be illegal. Bounty hunters offer a model for how contractual authorization can be used to selectively allow for certain defensive measures to be undertaken by qualified private actors. To be clear, this does not necessarily entail the cyber equivalent of knocking down doors and taking criminals into custody, but it could be applied selectively to enable limited action to attribute, disrupt, or mitigate ongoing malicious activity. Constraints on such activities through requirements imposed by the contractual relationship between service providers and end users, in combination with barriers to entry in the form of licensing authority granted by the government to able parties, could help mitigate some of the risks of their employment.

To establish a similar right to intrude upon private networks and confiscate data, companies might add a clause to their End User License Agreement (EULA) that allows for impositions on systems used in cyber attacks by malicious actors.[54] In other words, abusing a product for criminal purposes would to some extent forfeit the actor's right against some form of intrusion or disruption of their own systems by the vendor. In this approach, third party systems being utilized by malicious actors may, by necessity, also be subject to limited intrusion or disruption. Such impacts may be justified by some measure of negligence in maintaining the security of systems (lack of patching, insecure practices, and so on). Of course, it would be egregious to allow every company with a EULA to exercise such a right. Similar to bounty hunters, this space could be limited to certain actors with sufficient capacity and, moreover, to only those whose location in the broader ecosystem gives them a unique capacity to mitigate malicious activity. For instance, cloud service providers are able to leverage some of the most sophisticated defensive measures (particularly with the incorporation of machine learning and artificial intelligence into defensive capabilities) and are increasingly critical to the security of a vast range of their customers' assets. Further, companies acting in this role would still be liable for damages from exceeding narrowly defined parameters.

While this legal tactic is not currently employed, likely due to public reprisal and reputational damage concerns, the language of many EULAs does hypothetically allow for such actions.[55] And some EULA agreements have already been used as a mechanism to allow (or seek court allowance) to undertake certain assertive forms of cyber defense. Furthermore, contract law has been used to facilitate botnet takedowns, with defenders undertaking such action claiming status as a third party beneficiary to justify seizing subdomains.[56]

Such contractual backing, combined with a verified theft (through beacon use similar to anti-theft devices), reference to the fresh pursuit framework, and insurance best practices (along with civil liability coverage for oversteps), could address concerns regarding self-help intrusions to retrieve stolen intellectual property. Contractual acceptance of impositions on systems used in cyber attacks may qualify a company acting in that capacity as authorized to enter a private network.[57] This may, in turn, motivate those operating such networks to ensure they are not abused for malicious purposes. Finally, it is worth considering whether this discretion given to vendors makes it more feasible and reasonable to hold them to a higher degree of accountability for preventing the abuse of their products (potentially through some degree of liability for failure to do so).

Private Investigators

The United States industry of private investigation and security services began in 1850 with the creation of Pinkerton's National Detective Agency in Chicago. Allan Pinkerton was a famous Chicago policeman, and in 1861 foiled an assassination attempt against then president Abraham Lincoln. This organization was regularly hired by government and private parties alike to pursue outlaws like Jessie James, Butch Cassidy and the Sundance Kid, and the Molly McGuire Gang in an era of generally underdeveloped federal and state level law enforcement. The Pinkerton Agency grew very quickly and was hired to protect railroads from theft as they crossed jurisdictions (often police forces did not have the manpower to secure train routes).[58]

Current legal regulation of private investigators (PIs) is at the state level. While bounty hunters perform their tasks after an initial arrest, private investigators carry out investigative tasks on behalf of clients. PIs do not receive any special legal treatment when conducting their duties. However, licensing is much more widespread than that of bounty hunters—as of 2014, only four states do not require a PI license.[59] It is illegal for a PI to pretend they are someone else to get nonpublic information, or take recordings of individuals in circumstances with a reasonable expectation of privacy.[60] In most states, obtaining insurance is required as a condition of licensing.[61] Again, these insurance plans' specifics show the common liability risks of a private investigator. E.R. Munro &

Company, for example, is a PI insurance company that operates in all fifty U.S. states and provides specialty coverage for both bodily injury to others and property damage.[62] In another example of rule-setting by insurance companies, California law states that any PI using a firearm must have a $1 million insurance policy to obtain a license.[63]

Like bounty hunters, this analogy offers a potential model of how to create barriers to entry for certain measures through a combination of licensing and liability. Private investigators operate in a space parallel to law enforcement. They also, again, hold no additional legal powers or exemptions. This framework could be applied to actors engaging in cybersecurity measures that are preventative or investigative/anticipative in nature, similar to the security camera analogy and traceback techniques that use public routers. Behaviors of this type will likely yield high levels of civil liability from the general populace if they are not passive in nature, and as a result will require strict insurance policy requirements (similar to a PI's coverage for bodily harm or property damage). This would, in turn, empower insurers to constrain behavior by defining the necessary precautions and limits to engage in such measures.

Domestic Private Security

Private security contractors (PSCs) typically are not corporate employees or state agents but rather specialized subcontractors that provide comprehensive or ad-hoc security services on a contractual basis. Importantly, if a PSC is operating in the United States and employed by a private organization, then the legally permissible extent of their actions is far more limited than actual government forces. PSCs are only authorized to use reasonable force in the protection of property and apprehension of a perpetrator. Their mandate may be slightly increased by preexisting arrangements deputizing the contractor with police authority, however even in those situations lethal force is only authorized when a life is at risk, not property.

The nature of PSCs' activities entails a trade-off of countervailing risks. While charged with the protection of valuable private property, they are limited in their employment of defensive force that could harm others. They lack the legal authorization needed in many cases to undertake sufficient defense against attackers who have far greater freedom of action. This exposes PSCs (and their clients) to potential physical harm, making it likely that they will cross the line in the course of their duties. Consequently, PSCs typically face significant legal risk and must obtain extensive insurance coverage against lawsuits claiming that they surpassed their legally authorized reasonable force threshold. Brownyard Security, the largest U.S. insurer of PSCs, offers coverage for assault and battery, property damage, personal injury, false arrest, invasion of privacy, libel, and slander.[64]

Cybersecurity service providers offering specialized defensive services may operate similarly to private contractors who provide physical security. It is worth contemplating the circumstances in which such services might include measures impacting external networks that could harm third parties. When these measures are deemed necessary, some level of government authorization could help offset civil liability concerns. But as in the physical world, it will be critical to define an appropriate level of discretion given to defenders.

This demonstrates the inevitable trade-off of risks associated with self-help—constraining the defender's freedom of action may limit potential third party harm but exposes the defender and its clients to greater risk. Reasonable force has emerged in the physical realm to determine the permissible level of action a PSC may use directly against a threat actor. However, in the cyberspace context such a proposition is complicated by the potential for threat actors to be intertwined with third parties whose networks they use to perpetrate malicious activity. A reasonable force standard in cyberspace necessitates contemplating what level of harm to third parties is normatively acceptable.

This analogy underscores the role that insurance can play in resolving this challenge presented by the countervailing risks of aggressive self-help activities. Insurance can enable a balance that allows for viable defense while redressing the negative consequences for third parties when defenders cross the line of reasonable conduct. Moreover, when empowered to undertake this role, insurers can directly motivate contractors (through premiums and policy exclusions) to take necessary precautions and risk management measures that they calculate as necessary to minimize risks associated with their activities.

The potential transnational impacts present a significant complicating factor that makes it difficult to formulate insurance policies that cover such aggressive representation. The impacts of such measures across state borders might expose companies to legal ramifications or other forms of retribution internationally. Consequently, the consideration of appropriate boundaries of reasonable conduct for contractors in this domain must go hand in hand with the discussion in the next section of international systems of self-help governance in cyberspace.

Ex Parte Temporary Restraining Orders (Clothing Counterfeiters)

Rule 65 of the Federal Rules of Civil Procedure allows for a party to obtain a temporary restraining order against a malicious actor, without official court notice, if they can prove that immediate and irreparable harm will result without government assistance and that they have attempted to provide the other party with notice.[65] However, it has historically been recognized that any attempt to give

notice may make prevention of harm and/or prosecution of a crime fruitless. In 1979, the 2nd Circuit Federal Court ruled that an ex parte temporary restraining order (one without any notice to the offending party, official or otherwise) was necessary to make sure that a counterfeit clothing scheme could be cut off before the evidence was shifted to unknown affiliates.[66]

This approach has more recently been legally applied to botnet domain takedown efforts.[67] Specifically, Microsoft has sought ex parte temporary restraining orders to remove access to domains that are known to control botnets.[68] Similar to the clothing counterfeiting analogy, any notice to the controllers of these domains would allow them to create new and unknown access points to their botnet; thus an ex parte injunction is appropriate. In its takedown of the Citadel botnet, Microsoft went so far as to secure permission to send configuration files to infected computers without users' explicit consent and temporarily block internet access for some users in order to motivate them to remove the infection.[69] However, this operation was conducted under specific, court-approved parameters and in coordination with the U.S. Federal Bureau of Investigation and foreign counterparts.

This is a systematic approach that could potentially be applied to a range of defensive activities whose success depends upon their immediacy but that cannot be undertaken without express government authority. Certain ICT companies occupy unique positions to take action on behalf of themselves and the wider public, and they could be given limited authorization to do so when the circumstances do not allow for an effective law-enforcement-driven response.

This framework can be calibrated to account for a number of thresholds that narrow the space for engagement in such activity. As seen in the arguments put forth by Microsoft in various cases of botnet takedowns, authorization could be contingent upon demonstrating the benefit to broader public interest of mitigating malicious activity, the necessity for an immediate response, and the efficacy of the response, including that capabilities are properly tested and controlled.[70] Moreover, this allows for varying levels of law enforcement oversight and the imposition of liability for harmful impacts to third parties.

Private Self-Help in the International Context

Analogies from the U.S. domestic context illustrate boundaries that emerged and solidified to guide reasonable self-help and govern private actors undertaking roles complementary or supplementary to law enforcement. Yet cyberspace introduces unique complications for traditional approaches to domestic governance. Behavioral norms are being negotiated and asserted in an international

context. Decisions to set domestic rules for self-help in cyberspace have inevitable international ramifications. Domestic policy dilemmas are thus compounded by the lack of clear international rules and norms and, more fundamentally, diverging views of the proper role of states and private actors in the provision of security.

In this respect, self-help in cyberspace presents similar challenges to navigate as private physical security services in the international context. Private actors operate across state lines, often in semi- or ungoverned spaces. Global market forces and threats shape industry behavior in ways that can subvert national regulations. These factors generate tensions between states with diverging views and within states' domestic and foreign policy imperatives. The experience with private violence in the international context is thus invaluable for anticipating and navigating the emerging challenges associated with global cyber activities. However, for reasons described above, the focus here is not on international law pertaining to private self-help activities in cyberspace. Others have made strides in exploring this subject.[71] Rather, this section explores insights from the processes and mechanisms that emerged through unilateral and multilateral efforts to shape the reality on the ground regarding the behavior of private actors in security capacities.

Unilateral State Management of Private Use of Force

Any approach to governance needs to appreciate that cyberspace remains in a transient state. Before exploring the context of the modern, globalized private security industry, it is useful to briefly consider the roots of current norms and practices in the formative experiences with states' approach to private violence in the international context. This includes the practices of privateering and charter companies.

There are obvious limitations on the applicability of these experiences for instruments of governance in cyberspace (though letters of marque remain relevant). They nonetheless have important value, as Florian Egloff argues, for understanding "the long-term evolution of security dynamics in a space that becomes more important to stakeholders over time."[72]

Charter Companies

The rise of chartered companies around the sixteenth century has had lasting significance in both the precedents it set for private sector governance and the pivotal role it played in European imperial

expansion, and thus in shaping the contemporary international order.[73] Examples include the English East India Company, Dutch West India Company, and Hudson Bay Company.

Royal charters (and other variations) were used to sanction companies' efforts to marshal private resources toward ventures abroad that benefited the state. At least initially, chartered companies were driven by primarily financial interests in establishing trade and exploiting natural resources and indigenous populations in areas beyond the reach of states' relatively modest capacity. This entailed a significant degree of autonomy for companies operating in distant frontiers. Charters often granted companies powers and privileges on par with states—including to govern territory, conduct diplomacy, and even engage in warfare. "In their very constitution," Andrew Phillips argues, "they confounded the notions of territorial exclusivity and the compartmentalization of power into distinct public and private spheres."[74]

The mercantilist character of geopolitical competition among European states was crucial in shaping these practices. War and commerce were considered inseparable, and thus promoting commercial activities was not simply economically beneficial to states but a crucial element of interstate competition.[75] Charters offered an easy way to leverage private financial incentives and capacity under state auspices at a time when few other mechanisms existed to do so. They also were an attempt to place the burdens and risks of overseas expansion upon private capacities rather than sparse state resources.

Chartered companies grew to become tremendously powerful. Hudson Bay Company alone was, at its peak, "the largest landowner in the world," with close to 3 million square miles of North America under its control.[76] They relied almost exclusively upon their own means of security and commanded private police and military forces that in some cases rivaled or exceeded those of states. The English East India Company, for instance, commanded a force larger than the British Army in the late eighteenth century.[77] By empowering companies to engage in self-help, states absolved themselves of the burden of securing expansive commercial activities and could (to some degree) dissociate themselves from the violence required to do so.

Suffice it to say that there are obviously vast differences between charter companies and contemporary corporations. But it is worth considering the parallels in these formative experiences. Cyberspace is in the midst of a "frontier era," argue Chris Demchak and Peter Dombrowski, in which "the underlying technological layer is itself changing as are the social structures depending upon cyberspace."[78] Individual companies maintain and control large swaths of territory at each layer of cyberspace[79]—from physical infrastructure to software platforms and content. States have largely encouraged this unimpeded expansion into the domain—indeed, ICT companies' commercial

success has often been a matter of national interest. At the same time, states are struggling to protect their own assets and find their authority attenuated by the inability to sustain a presence throughout this frontier. Consequently, corporations have enjoyed the benefits of autonomy but have largely been left to their own devices to manage their risks.

Given this state of affairs, the experience with chartered companies serves as an admonition against granting the private sector complete leeway to exercise self-help in cyberspace. But the deeper insight is seen in the circumstances that gave rise to self-help and the challenges states faced when attempting to reassert their authority over the space. As perceptions of the advantages and liabilities of chartered companies shifted and states sought to bring them under more direct control, they were forced to devote significant resources to their protection and at times provide a financial lifeline to companies for "ill-conceived and profit-less colonial adventures."[80] States' assumption of responsibility for the vast possessions of these companies translated into a dramatic expansion in their imperialistic behavior. This was at some level unavoidable given how far the companies had expanded into this new frontier.

What would it entail for states to similarly assert their authority over governance in cyberspace and attempt to monopolize force? And in a domain dominated by major multinational corporations, how would states begin to demarcate the extent of their responsibility for the provision of security?

Letters of Marque

Privateers were privately owned and operated ships that were given a limited authorization by a state to effectively commit acts of war at sea and reap financial benefits. The practice of privateering emerged as early as the thirteenth century at a time when the maritime domain was a largely ungoverned space, state capacity was weak relative to private actors, and threats to commercial entities were proliferating. Merchant ships armed themselves to undertake their own protection—and retaliation. Authorization of privateering came in the form of a letter of marque and reprisal, which generally allowed a privateer to attack and seize the property of any vessel of the adversary nation to compensate for losses.[81] Such letters were also issued in peacetime to provide for limited authorization for a privateer to hunt down a pirate after being attacked.[82] In doing so, letters of marque provided a mechanism for states to empower private actors to engage in self-help while advancing their own strategic and economic objectives.

At a time when states' navies were nascent, letters of marque were a tool to harness and direct privately held capabilities toward state ends—enriching the state and conducting warfare without

drawing upon state resources. At times, privateers even functioned as reserve navies, as was the case when the United States called upon privateers to help defeat the British siege on New Orleans in 1815. Privateers were a product of a period characterized by mercantilism, when such attacks on commercial entities were accepted as legitimate tools of statecraft. The interests of the state and of its commercial entities were blurred, and enabling this kind of self-help advanced both.

Over time, however, the calculations of states shifted, and the system of privateering appeared increasingly detrimental to stable maritime commerce. Eventually, this led to the abolition of privateering at the Congress of Paris in 1856, largely driven by Britain, then the preeminent maritime power.[83]

It took hundreds of years for a state of law and order to emerge and supplant reliance upon self-help. The balance between state and private actors' roles in this space was slow to evolve. Even as states gradually consolidated naval power, it proved difficult to impose their authority over the space, where norms of self-help behavior had solidified. An inflection point occurred when Britain concluded that privateering had come to undermine its interests. Even still, Britain had to motivate smaller powers that continued to benefit from the practice, such as the United States, by assuming greater responsibility for securing the domain for private actors.[84]

Letters of marque offer a potential template for how states could selectively authorize the use of certain defensive measures against attackers that would otherwise be prohibited (like those with impacts outside of the defender's network). The inability of governments to provide sufficient defense to the private sector and the significant potential of aggressive self-help measures to shift the balance in favor of defenders have caused this idea to gain some traction.[85] For instance, Dave Aitel argues that cyber letters of marque offer a scalable solution to evolving threats.[86]

A realistic application of letters of marque to private sector self-help in cyberspace would necessarily be far more limited than the broad leeway given to naval privateers to target enemies of the state. Such limitations could take the form of restrictions on tactics or measures employed or the scope and duration of effects. Authorization could be granted to private actors to undertake action to mitigate persistent intrusions, such as the aforementioned poisoning the RAT. Alternatively, letters of marque might preauthorize defensive action against a particular threat actor in the event of a future attack, such as the use of white-hat ransomware. There are already signs that states are exploring such options in the cyber domain. Singapore, for instance, has adopted a legal mechanism for sanctioning private entities' defense of critical infrastructure (though it remains to be seen how it will be employed in practice).[87]

However, the potential pitfalls of this approach need to be seriously examined. If used to authorize aggressive defenses (or even offensive measures such as hacking back), they would contribute to perceptions that states are employing proxies toward their own ends. Moreover, the justification of the necessity of some aggressive measures would be questionable in any case. As critics of hacking back have pointed out, if an attack has successfully exfiltrated data it takes very little time for that data to then be copied or distributed. Outside of a narrow window of opportunity to respond to mitigate damages, hacking back has dubious benefits for the defender. Thus the challenge of an approach based on letters of marque would be how to tailor it specifically to contexts of defensive necessity while at the same time making the process itself rapid enough to deal effectively with threats.

Finally, cyberspace is not the high seas, and letters of marque offer no solution to the problems of defensive measures that violate the domestic laws of another country. Moreover, the historical experience with letters of marque offers an admonition against purely unilateral solutions. In the absence of any international understanding of the scope of legitimate self-help measures or mechanisms to resolve disputes regarding violations of domestic laws, cyber letters of marque would exacerbate tensions in a domain already characterized by behavior reminiscent of mercantilism, including widespread commercial espionage. States will have diverging views on the legitimacy and legality of certain actions. If each state chooses where it draws the line for its own companies, the potential for systemic escalation could be high. Thus, significant multistakeholder dialogue and convergence upon international norms would be needed to contain the risks of a dramatic expansion of these activities, in order to prevent destabilizing consequences.

Nevertheless, a modern day version of letters of marque tailored to the context of cyberspace might offer an effective, temporary solution by which states could allow for self-help within narrowly defined parameters while retaining the ability to rein in such behavior. Albeit this is a solution more to the problem posed by states' own domestic laws, not to the trade-offs and risks posed by the activities themselves. The potential flexibility and adaptability of this tool is attractive for overcoming two significant policy challenges regarding self-help in cyberspace: The need for evidence of the efficacy of many potential measures that could be employed and the need to condition self-help to some degree upon the capacity of a defender to undertake responsible conduct. Any blanket approach to self-help in cyberspace would be problematic. Specific kinds of entities like ISPs and cloud service providers will have unique opportunities and responsibilities to defend themselves and others, and letters of marque could be tailored to these unique circumstances.

International Multistakeholder Initiatives Governing Private Security Contractors

States appear to be increasingly employing cybersecurity contractors for both defensive and offensive cyber operations in a manner that has already prompted comparisons to private military and security contractors (PMSCs).[88] In one notable example, a former director of the U.S. National Security Agency, General Michael Hayden, used the term "digital Blackwater"—referring to the controversial U.S. PMSC whose employees were convicted of killing fourteen Iraqi civilians in 2007—to suggest where current trends might lead.[89]

Whether or not it is desirable to have a global industry of cybersecurity providers engaging in measures equivalent to use of force in cyberspace, the challenges and potential solutions for governing such an industry must be considered. The parallels between PMSCs and the rapidly expanding and consolidating industry of managed cybersecurity services[90]—including growing evidence of a transnational market for aggressive self-help services—suggest that the historical and contemporary experience with PMSC governance holds valuable insights for both anticipating the trajectory of these services and finding practical solutions to shape that trajectory.

The Montreux Document

The resurgent role of private actors in the provision of security since the end of the Cold War has been driven by a diverse range of factors. States themselves have actively fueled the rapid expansion of a global industry of PMSCs from a variety of motives.[91] Some states turn to private capacities to supplement thinly spread public resources. Others see the benefit of using contractors to enable militaries to maintain a light footprint in theater or allowing officials to distance themselves from controversial practices. In some cases, PMSCs operate under more relaxed rules of engagement than military forces precisely for this reason. While states' employment of PMSCs is distinct from private self-help, it has direct bearing on legitimizing and empowering contractors to provide self-help services. Moreover, the close relationship between states and PMSCs in many cases blurs the lines between states' and private actors' interests in protecting private assets.

Concerns over the lack of accountability or effective governance of PMSCs internationally long predate the incident involving Blackwater in Iraq. As the industry began to rapidly expand in the post–Cold War environment, many countries lacked effective regulations on PMSCs operating from or within their territory. The ability to outsource services to the international market of PMSCs made it easy to circumvent domestic regulations in states that had them. In the absence of progress toward an international regime for managing the employment of PMSCs, a multistakeholder

initiative was launched in 2006 by the Swiss government and the International Committee of the Red Cross to bring clarity to the rules regarding state responsibilities for PMSCs. This initiative brought together states (including some of those most affected by PMSCs), NGOs, industry representatives, and academic experts with the modest initial objective of assessing the applicability of existing international law to states' regulation or employment of PMSCs.[92]

This initiative resulted in the "Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies During Armed Conflict" (often referred to simply as the Montreux Document). It was finalized on September 17, 2008, with seventeen states initially signing on.[93] Since then the number of state participants has risen to fifty-four.[94]

The Montreux Document set forth voluntary guidelines for how states should manage their relationships with PMSCs to ensure their compliance with international law, including international humanitarian law (IHL) and human rights law, and minimize the risks of negative consequences from their activities. This included a set of best practices for the employment of PMSCs. These range from criteria for vetting and selecting contractors to procedures for authorizing their conduct to monitoring compliance and responding to misconduct.

Three primary categories of state relationships to PMSCs are delineated: contracting states (those employing PMSCs), territorial states (on whose territory PMSCs are operating), and home states (where PMSCs are based). Each of these categories entails specific obligations with respect to preventing and remediating PMSC misconduct. For instance, the Montreux Document applied contracting states' obligations under IHL not to contract out activities that are "non-transferable responsibilities of the State," such as the supervision of detainee facilities.[95]

The Montreux Document offers a model for state accountability for private actors building on states' commitments under international law. There is a growing consensus that states are responsible for nonstate activities occurring in or through ICTs in their territory,[96] but fundamentally conflicting views have impeded any progress toward an understanding of what this entails in practice. The Montreux Document provides a useful conceptual starting point underscoring a number of questions regarding states' responsibilities for private self-help activities: What kinds of cyber operations should be the exclusive domain of agents of the state (akin to "nontransferable responsibilities of the state")? Should territorial states be further separated into those where cybersecurity service providers are physically operating and those states whose ICT infrastructure is being used for cyberspace operations? What level of authorization should be required for private

entities operating from or through a state? In any case, what kinds of mechanisms and precautions should be taken to prevent or remediate misuse of a state's ICT infrastructure?

The Montreux Document also demonstrates various mechanisms states can employ to ensure responsible conduct within the space of activity considered legitimate. For instance, it includes PMSC selection criteria that is aimed at discouraging states from hiring contractors likely to engage in risky behavior—contractors' past records of criminal activity, financial capacity for liabilities, and the status of licenses and registrations, among other factors.

The PMSC experience underscores the importance of addressing the asymmetries in states' approaches that allow for gaps in governance to emerge. Converging upon an international understanding of the boundaries of legitimate employment of private contractors and the responsibility of states for their actions could begin to address the broader issues surrounding states' use of proxies for cyber operations. Setting forth specific requirements that states ensure that contractors are not engaging in activities in violation of laws or exceeding the authority granted to them would make it harder for states to turn a blind eye to private entities conducting illegal activities.

International Code of Conduct for Private Security Service Providers

The Montreux Document addressed only one dimension of PMSC governance—the role of states as both regulators and clients of PMSCs. However, efforts directed at states could only go so far in holding private actors accountable. A complementary effort was needed toward the PMSC industry itself. Thus, the Montreux Document paved the way for an initiative that sought to apply the same principles to the industry directly, in the form of a voluntary code of conduct. Finalized in 2010, the International Code of Conduct for Private Security Service Providers (ICoC) expanded upon the principles in the Montreux Document and established additional provisions to guide PMSC conduct. The ICoC has since been successful in gaining commitments from over 700 companies worldwide.[97]

Like the Montreux Document, the ICoC includes many practical measures to minimize risks, such as properly vetting and training personnel (particularly with regard to the use of firearms). Training must be specific to the type and model of weapon, and must be "regular, verifiable, and recurrent." It also includes measures in the event of misconduct, such as requirements for incident reporting and grievance procedures. These measures were supplemented by the creation of an internal,

independent oversight mechanism for monitoring and certification of companies' compliance, which was formally agreed upon in 2013.[98]

The application of principles of necessity and proportionality to the use of force included in the Montreux Document are elucidated in greater detail in the ICoC. PMSCs are required to "take all reasonable steps to avoid the use of force." Force should be limited to "what is strictly necessary" and "should be proportionate to the threat and appropriate to the situation." Moreover, personnel are prohibited from using firearms except "in self-defence or defence of others against the immediate threat of death or serious injury, or to prevent the perpetration of a particularly serious crime involving grave threat to life."

As in the case of PMSCs, successful governance of cybersecurity services will depend on engaging those in the industry providing such services to help craft effective and realistic rules.[99] The ICoC offers a corporate social responsibility (CSR) model for exploring the proper precautions, rules of engagement (ROEs), and other risk-management measures that could be directly applied to the emerging industry of cybersecurity service providers.[100] Some of the specific provisions are readily translatable to the context of managed cybersecurity service providers: Ensuring that contractors are following applicable international and national laws, properly vetting personnel, and establishing procedures for incident reporting and disciplinary action. Similar requirements could be established to ensure that certain capabilities are controlled and the personnel employing them are thoroughly trained.

In other cases, the ICoC offers principles that could be adapted to the unique circumstances of self-help in cyberspace. The requirement that all reasonable steps should be taken to avoid having to resort to aggressive defense would entail robust passive defense before more assertive measures are taken. Capabilities that pose any risk should be limited to situations of necessity and proportionate to the threat facing the defender. Such guidelines could factor in thresholds for attribution required to undertake certain measures. Further exploration of how these principles would apply to specific scenarios of self-help in cyberspace is needed.

A corporate social responsibility approach can fill a unique niche in a broader effort to shape the incentive structure for the private sector. Governments and industries could include adherence to a code of conduct as a contractual requirement, as many do in the case of PMSCs. Even in the absence of such requirements, there would be strong reputational incentives should a code of conduct be promulgated. Daphne Richemond-Barak argues that the PMSC industry's participation, rather than resulting in watered down standards, led to the adoption in some cases of best practices and

standards that exceeded legal requirements. The industry's participation had an overall effect of increasing security providers' investment in norms, creating a self-reinforcing legitimacy.[101]

Voluntary Principles on Security and Human Rights

The Montreux Document and ICoC were complementary in attempting to shape industry behavior through both directly within the security sector and indirectly through governments. But equally influential in shaping PMSC behavior are the private industries that contract for security services. They were the focus of a separate initiative that actually preceded the Montreux Document and ICoC. Established in 2000, the Voluntary Principles on Security and Human Rights (referred to as Voluntary Principles) were a joint initiative of the UK Foreign and Commonwealth Office and the U.S. Department of State aimed at the practice of security contracting by extractive industries.

Extractive industries—including oil, gas, and mining companies—comprise a significant portion of the global demand for private security services.[102] They frequently operate in developing states where there is potential for violent conflict and state capacity and authority are limited, creating a need to supplement public security. At the same time, corporations' home states often eschew responsibility for commercial activities in complex security environments outside of their territory—whether to avoid the financial costs and resource commitments or to distance themselves from the political ramifications of potential violence. Even countries with a deeply rooted aversion to private violence have turned to PMSCs to secure extractive industries abroad.[103] In such complex security environments with weak rule of law the potential for human rights abuses by private contractors is high. The Voluntary Principles initiative was in part a response to incidents of abuse by PMSCs employed by extractive companies.[104]

Sharing the same basis in IHL and human rights law, many of the provisions of the Voluntary Principles closely resemble those contained in the Montreux Document and ICoC, but the responsibility is placed upon extractive companies to ensure appropriate conduct of PMSCs they employ. Companies are obligated to properly vet personnel, report incidents, and take disciplinary action in the event of misconduct by a contractor. Similar safeguards to protect human rights and limits on the use of force to cases of necessity are recommended for inclusion in contractual arrangements with PMSCs. Additionally, the Voluntary Principles set out guidance for the conduct of risk assessments by companies, including factors in the environment where they are operating and risks with respect to their activities, such as transfers of lethal equipment.[105]

If the ICoC offers a potential CSR template for cybersecurity service providers, the Voluntary Principles offer a complementary template for those driving the demand for cybersecurity—in particular, the financial, ICT, energy, and other relevant sectors—to shape responsible self-help practices. The Voluntary Principles underscore the critical importance of the demand side of the equation in shaping the behavior of security providers and managing the risks of their activities.

Those entities driving the demand for security are in a unique position to enforce behavioral norms because they contribute significantly to the capacity and legitimacy of security service providers. As Rita Abrahamsen and Michael Williams argue, the private security industry "derives considerable power from its connection to clients and from their view of the provision of private security as a legitimate and necessary aspect of their operations and daily life."[106] In other words, the legitimacy of private contractors' services flows from the legitimacy of their clients' property rights, which governments are increasingly unable to protect in the context of global commercial activities. If these stakeholders determine certain activities are out of bounds, they can use their market power to motivate security providers to abide by such norms. And through their contractual arrangements, procurers of services can directly apply constraints to self-help conduct and hold contractors accountable for misconduct.

Moreover, those entities whose property is the focal point of both offensive and defensive efforts have significant ability to proactively shape the risk landscape. This includes properly assessing and minimizing risk exposure in the first place. The Voluntary Principles' guidance on risk assessment aimed to shift behavior toward minimizing risk rather than simply channeling it outward. Cyber risk management should likewise begin with preventive measures corporations can take to protect crucial data, mitigate vulnerabilities and attack vectors, and secure their networks that may obviate the need to resort to defense.

The fact that cyberspace is to a significant degree owned and operated by private companies creates an inescapable dilemma for governments that value both property rights and their control over the use of force in cyberspace. Governments cannot undertake cyber defense in any comprehensive manner without intruding deeply into private property that is itself increasingly incongruent with national boundaries. Private actors thus enjoy relative advantages in their capacity to provide for cybersecurity not just from their technical capabilities but also from the extension of legitimacy to their activities via property rights and contractual agreements (for example, EULAs). This makes it essential to consider how to leverage the key industries whose networks will be the key battlegrounds to establish and enforce norms for self-help.

Market-Based Mechanisms for Regulation

Self-Regulation of Private Maritime Security Contractors

When the proper financial incentives for risk management are in place, self-regulation can partially fill the gap left by the absence of state efforts, and norms can emerge organically as outcomes of the forces acting upon the private sector. Here, an instructive experience is the evolution of norms for the employment of armed guards by the maritime shipping industry in response to the escalating threat from Somali pirates in the late 2000s.

The rise of Somali piracy affected roughly one-quarter of global maritime trade. While security of the contemporary maritime shipping industry had been viewed by governments and industry alike as the responsibility of states, this consensus began to erode as huge naval deployments proved unable—and partially because of their rules of engagement, unwilling—to ameliorate the deteriorating situation in the Gulf of Aden. Between early 2008 and early 2009, the number of attacks increased about 300 percent.[107] Facing a growing existential threat to business from hijackings and a lack of viable alternative measures, the shipping industry turned increasingly to armed guards for defense against pirates.

A thriving market of private maritime security contractors filled the demand for security, initially with almost complete absence of government oversight. What regulations were in place could be circumvented by the ability of ships to sail under flags of convenience (that is, they were registered to those states with minimal regulations) and operate in international waters.

Naturally, many states were ambivalent about the growing practice. Even those less averse to the privatization of force in general had significant concerns over violent self-help measures, including the potential for escalation and collateral damage. Yet precluding this form of self-help required more than a simple prohibition of the practice. It would have required addressing the forces driving the practice—namely through either far more aggressive and sustained naval action or, in its absence, some means of offsetting the massive costs to industry.

However, despite serious concerns of a race to the bottom in the industry, with contractors resorting to risky and reckless behavior in a bid to offer the most successful anti-piracy services, norms of responsible conduct emerged to govern contractors' behavior. This was driven in part by the insurance industry, which recognized both the benefits of armed guards (no ship with armed guards had ever been hijacked) and the need to constrain the potential risks of their activities. The insurance industry worked with the Security Association for the Maritime Industry (SAMI), established in

2011, to promote a set of standards for armed guards that it could incentivize through the cost of insurance premiums. This was complemented by broader industry guidance on best practices for the employment of contractors, such as that issued by the International Maritime Organization.

These standards were aimed at minimizing the risks of the use of potentially lethal force, which had become an unfortunate necessity. This included specific precautions to prevent escalation and collateral damage such as ROEs, including adopting a "graduated level of deterrence, at a distance."[108] Thus, while lethal interactions could not be ruled out entirely, standards guided behavior toward minimizing the negative consequences, such as by disabling an attacking ship's engine rather than firing directly at pirates. The complementary incentive structures within industry helped prevent systemic escalation; in the long run, the adoption of armed guards did not produce a vast increase in the human costs of piracy, but instead created a deterrent that contributed to piracy's dramatic reduction in the region.

The maritime security analogy offers practical insights into how the cyber insurance industry, by itself or in partnership with industry associations, can play a crucial role as a proxy regulator of self-help activities. The growing cyber insurance industry has both the analytical potential to determine responsible self-help conduct (as data from experience is accumulated) and the ability to motivate corporations to remain within such boundaries.[109] This would include determining and ruling out those cyber measures that would be too risky to underwrite (such as those that could cause physical harm) while predicating engagement in other measures upon steps to minimize their risks.

This could mirror the insurance industry's partnership with SAMI to motivate maritime security contractors to take necessary steps to manage risk, from vetting employees to abiding by responsible ROEs. Similarly, the largest international shipping association, BIMCO, developed a standard contract widely used by shippers for hiring PMSCs that explicitly seeks to weed out unqualified guards that would put ship owners and crews at risk by setting high requirements for insurance coverage and proper licensing and permits for weapons.[110]

Given the limitations on states' abilities to effectively contain cyber threats or regulate a transnational market of cybersecurity service providers, insurance provides an attractive option for formulating and incentivizing norms of responsible conduct. Instead of a top-down imposition of norms for self-help behavior by states, the maritime experience demonstrates how industry self-regulation can reshape states' approaches. SAMI served as the basis for industry standards codified in ISO 28007 and the 100 Series Rules for the Use of Force. These were in turn adopted by national approaches, such as the United Kingdom's approach of voluntary regulation of PMSCs.[111] Contrary to the expectations of some that private violence entailed an irrevocable loss of state sovereignty, PMSCs arguably

enabled state authority and control over a chaotic space by halting a rapidly deteriorating situation and, in turn, giving states breathing room to bring the practice of maritime security under the fold of regulatory frameworks.[112]

Key Takeaways

Each analogy examined here illuminates a point at which state responsibility ends and private actors turn to their own means for security or contribute more broadly to ordering an environment. Collectively, they reveal the extent to which states' monopoly on the legitimate use of force in the physical world has been historically and remains qualified in practice. The extension of this trend into cyberspace presents novel dilemmas for policy. However, the core challenge of striking a balance between the roles of government and the private sector is a perennial one for states in the modern era.

There are benefits and pitfalls with these analogies. A study focusing primarily on the U.S. domestic context as well as a handful of salient international examples has obvious limits to its generalizability. A more important caveat is the difficulty with the very conceptualization of force in cyberspace. The character of many of these cyber measures does not lend itself to simple comparisons with physical force. Finally, any single analogy captures only part of the broader challenge. The rules governing these cyber activities must address both the domestic and international dimensions of the space. For these reasons, rather than dwelling on any one, a broad survey of analogies has been drawn upon to explore individual and collective insights.

Despite their inherent limits, these analogies have heuristic value for considering the boundaries of self-help in cyberspace within a broader understanding of how states govern forceful self-help activities. It is useful to start by mapping the varying approaches to governance along the rough gradation laid out previously in Figure 1.

States restrict certain activities considered unequivocally outside the remit of legitimate self-help. Most notably in the domestic context, this includes lethal defenses and other measures that pose inordinate risks to human safety. Within those absolute limits, however, lie many cases in the middle of the spectrum—activities tolerated, tacitly condoned, or explicitly encouraged and supported by the government. In the international context, states often exercise loose oversight of private actors and the distinction between state and private roles often becomes blurred.

These different approaches speak to the diverse rationales underlying states' approach to self-help. Understanding these rationales is important to anticipate how states might or should approach comparable cyber activities. Four rationales recurrent throughout these historical and contemporary experiences are worth underscoring here for their relevance to the cyber context:

States desire to harness unique private sector capacities: States may look favorably upon private activities that fill a unique role in combating malicious activity or alleviate the demand placed upon public resources. Private actors' physical and temporal proximity to malicious activity creates fleeting opportunities to intervene that justify their immediate response, as in cases of citizen's arrest or fresh pursuit. Private entities can also exercise control over their property to minimize exposure, reassure themselves of their security, raise the costs and risks of criminal activity (possibly through perimeter defenses), or interfere directly with criminal acts (for example, through booby traps).

Evolving technology enables new means of mitigating the impacts of crime and facilitating law enforcement responses, such as dye packs and anti-theft devices. Moreover, self-help measures that are difficult for criminals to anticipate or detect, and that make defenses less predictable and payoffs of attacks less assured, contribute to the general deterrence of criminal activity, to the benefit of both private actors and law enforcement. Lojack, for example, serves to deter car theft in general because it is harder to detect than a steering wheel lock that may only deter the theft of a single car, making the former a more attractive form of self-help to promote from a governmental perspective.[113]

This rationale can be even stronger when private actors enjoy significant advantages in expertise and capacity relative to states. In such cases, the private sector may enjoy far greater leeway, including even the employment of lethal capabilities. The most extreme example was the use of letters of marque by states to take advantage of private capacities to wage economic warfare. More recently, states have embraced the specialized services of private military contractors to deal with complex security challenges like piracy.

States seek to avoid responsibility for risks to private assets: States tolerate some forms of self-help they might otherwise reserve for public actors in part to avoid assuming responsibility for the risks created by commercial activities and the burden of protecting them (and to avoid creating a moral hazard). Private security contractors satisfy the growing demand for protection of private assets or commercial spaces like shopping malls in lieu of public resources. This partly explains the roughly 1.1 million private security personnel in the United States outnumbering 800,000 police officers—a disparity even more pronounced in other countries like India, which has 7 million private security personnel compared to 1.4 million police officers.[114]

Globally, states often eschew responsibility for securing the transnational activities of corporations in extractive industries, among others, and instead turn to private capacities. Even countries, like China, that are traditionally averse to privatization have come to rely increasingly on private security contractors for the protection of global commercial activities.[115] The reluctant acceptance of these activities often comes with constraints placed upon behavior short of proscribing it. For instance, states may raise barriers to entry in the form of licensing and insurance requirements for security contractors.

States find their authority or control over a space limited: The inability of states to actualize a monopoly over force often serves to legitimize self-help. This was most evident in formative experiences with chartered companies and privateers featuring states' encouragement and facilitation of private violence in part because of the sheer disparity between those companies' and states' own nascent capabilities.

In other cases, states are simply unable to prevent self-help they are otherwise averse to. Some states have been reluctantly dragged along by trends outside of their control such as the use of armed guards in the maritime context. For the same reasons they couldn't simply disarm pirates, states couldn't easily dissuade corporations from using armed guards in international waters.

States may be inclined to allow conflicts between legitimate private interests to work themselves out: Self-help often entails a clash between the legitimate interests of both defenders and third parties impacted by their defensive measures. Whether an action to protect property or personal safety is perceived as reasonable or justified often depends not only upon values and ideology but also on the expediency and legitimacy of its application in the particular circumstances of a given malicious attack—the perceived threat to a security contractor or the immediate need of a citizen to incapacitate another or trespass onto property.

As Douglas Lichtman argues, self-help allows for "diverse, individuated judgments" of how best to remedy malicious activity compared to blunter tools of governmental intervention.[116] Rather than attempt to set hard rules defining legitimate conduct in every circumstance, states may leave the space of reasonable behavior to civil litigation to shape. Criminal and civil liability play complementary roles in moderating behavior across shifting circumstances of self-help.

In practice, these four rationales shaping states' approaches to self-help are often difficult to distinguish. And of course, the frameworks that emerge to govern self-help cannot simply be accounted for by utility-based decisions. They are shaped by historical contingencies, societal values, political dynamics, and in some cases random events that produce broader shifts in perceptions. The

reining in of military contractors after the Blackwater incident is a case in point. Even within the United States, there is variance at the state level attributable to these different circumstances. These competing forces often produce indecision and equivocation rather than coherent policy.

Nevertheless, these interacting rationales tend to result in a balance along several dimensions:

- First, between the roles and responsibilities of public and private actors in the provision of security. Lines often emerge to demarcate where state responsibility for property begins and ends—though they do not always correspond with physical property lines.
- Second, between the protection of property and the risks of self-help, including, most importantly, to human safety. Bodily harm is often the point at which the leeway given to private actors becomes significantly curtailed (as in the case of perimeter defenses or PSCs).
- And third, between the rules imposed by a state domestically and those arrived at through international efforts. Limitations on state authority and control over transnational activities often necessitate some attempt to harmonize domestic rules with international norms.

These rationales are each visible in cyberspace to some extent. It seems reasonable to suggest that a similar balance along these dimensions is both likely and desirable from the standpoint of addressing the broader cybersecurity challenge for states and the private sector. But before turning to the insights from analogies for where and how to strike such a balance, the unique challenges of the cyberspace context must be noted.

Bounding Self-Help in Cyberspace

Striking a balance to govern private self-help in cyberspace demands an approach calibrated to its inherent characteristics that complicate governance: in particular, the blurred distinctions between foreign and domestic, and the dual character of cyberspace as a largely privately owned territory under national jurisdictions and, simultaneously, a de facto global commons.[117]

States seek to order their domestic cyberspace and set rules for private actors in their territory. Yet they find their ability to do so significantly attenuated, in part because they lack control over actions occurring within and through this space. Globally dispersed cyber threats lie beyond the ability of any one state to mitigate, and states cannot easily police cyberspace like they can their domestic territory. At the same time, individual corporations hold resources, capabilities, and expertise that rival or exceed that of many states. For instance, JPMorgan Chase spends more on cybersecurity than is allocated to the budget of U.S. Cyber Command.[118] Evidence is mounting that the private sector

is beginning to take advantage of the uneven regulatory environment internationally to circumvent limits on self-help.[119]

Moreover, the character of cyberspace as constructed and maintained largely by the private sector places inherent limitations on state control. This parallels numerous historical experiences in which private entities have largely been responsible for generating risk and, consequently, left to their own devices to manage it. This reality raises a fundamental question: Is it even possible (at this point) for states to assert sovereignty, monopolize force, and order cyberspace to the degree they do their domestic territory?

In the past, the ambitions of states to assert control over chartered companies that had extended far into distant frontiers translated into imperial expansion. It seems that the sort of presence in cyberspace that would be required to monopolize force would similarly entail some dramatic expansion of state control, or colonization, of the domain. What this would even look like in a globalized domain where multinational corporations may have systems and data in dozens of countries is unclear. But in any case, the current distribution of capacities in favor of the private sector suggests that this remains a distant possibility.

Consequently, private sector cyber activities may present states with similar challenges as the global security sector in the physical world has—not only to their foreign policy but to their aspirations to order cyberspace domestically. This should serve as an admonition against any unilateral approach toward this global governance challenge. One state's attempt to impose order of what it considers its cyber territory may interfere with others', particularly if this translates to tolerating or encouraging self-help activities with transnational impacts. An ultimate resolution to the issues presented by assertive self-help activities will require some convergence upon a conception of reasonable self-defense in cyberspace and state responsibility for private actors.

However, here it is essential to identify where the similarities between physical force and actions in cyberspace begin to break down. The various frameworks governing self-help in these analogies often reflect the unique characteristics of force in the physical world—in particular the risks of harm to humans. A lethal booby trap cannot easily be made to discriminate between intruders, abort or reverse its effects, or tailor its impacts to the minimal necessary to disrupt an intrusion. Yet such possibilities do exist in the case of certain cyber measures that are reversible or temporary, and they are worth exploring further in addition to the traditional mechanisms for moderating behavior and holding actors accountable.

Few scenarios involving the defensive measures discussed here include any risks to human safety. These risks could be addressed as they have been in the physical world (that is, through a combination of technical and circumstantial limitations and liability). Lumping the full spectrum of potential impacts on external networks into the category of "hitting back" vastly inflates the conception of force in cyberspace. More importantly, it may unnecessarily stigmatize measures that could not only benefit defenders but contribute to the broader stability of cyberspace. It seems conceivable to distinguish the characteristics and circumstances of reasonable from unreasonable employment of various active defenses and other measures. This suggests there is room to explore for international norms for responsible self-help.

Individual Insights From Analogies

The historical continuities and discontinuities presented by the cyberspace context illuminate both the value of these analogies and where their application begins to break down. The domestic analogies offer a range of insights particularly relevant for addressing four aspects of self-help (see table 1 as well):

1. low-risk/high-reward measures that could reasonably be encouraged by states (provided basic safeguards are in place);
2. high-risk measures that might be justified under narrowly defined circumstances and with significant constraints;
3. measures with highly variable risks, whose employment should be contingent upon other efforts to satisfactorily manage risks; and
4. specific mechanisms or approaches for creating barriers to entry and governing behavior.

Table 1: Applying Insights From Domestic Analogies to Cybersecurity

	PHYSICAL PRECENDENT	CYBER ANALOG	KEY TAKEAWAY
LOW RISK / HIGH REWARD	Public surveillance	Traceroutes and similar measures for intelligence gathering	Measures with limited intrusiveness into privacy can allow for greater situational awareness and attribution
	Electric fences	IP blocking; traffic deflection	Differentiate low-risk measures from those with potential harm to third parties external to the network
	Booby traps	Tarpits; honeypots	Internal network defenses should have little restriction but tight controls needed if measures exceed network boundaries
HIGH RISK	Castle doctrine; Stand Your Ground	Disruptive or destructive response (hacking back)	Direct and imminent threat to human safety might justify measures to disrupt an attack
	Citizen's arrest; fresh pursuit	Temporary trespass into or disruption of attacker networks; poisoning the RAT	Necessity of immediate response may justify a level of force (provided some standard of attribution is met)
VARIABLE RISK	Anti-theft devices	Beacons; white-hat ransomware	Automated disabling or location of stolen devices is feasible with basic safeguards
	Dye packs; credit card fraud	Corrupting stolen data; white-hat ransomware	Automatic measures with external network effects can be limited to verified thefts and nonharmful to third parties
TOOLS TO GOVERN BEHAVIOR	Bounty hunters	Contractual-based authorization (EULAs); licensing authority	Limited mechanism to authorize key stakeholders to mitigate the abuse of ICTs for malicious purposes
	Private investigators and security contractors	Cybersecurity service providers / investigators	Incentivize responsible conduct via requirements for insurance coverage and liability to cover investigative and defensive activities
	Ex parte temporary restraining orders	Domain seizure; botnet takedown or cleaning "infected" systems	Model for selective legal authorization for certain actors or actions against malicious activity

The international analogies offer similar precedents that could be applied to the employment of specific measures: principles for risk management, rules of engagement, and so on. But their more salient contribution may be in illuminating the hallmarks of a successful *process* for governance in the context of an ever-changing security landscape and transnational markets for security services.

First, there needs to be some effort toward harmonization of states' approaches to governance. Much can be done by states unilaterally to govern self-help. Mechanisms like letters of marque offer potentially useful tools to unlock private capacities and address the immediate demand for security. However, early experiences with chartered companies and privateers demonstrate the pitfalls of such unilateral solutions. Some basis of common understanding and remediation is needed, beginning with those activities that should be considered equivalent to "non-transferrable responsibilities of the State" as discussed in the Montreux Document. And given the fraught state of cyber norm-building efforts at the United Nations and elsewhere, a more modest initiative akin to the Swiss-led process may be more promising for making progress on answering such questions. Multistakeholder initiatives can have intrinsic value simply by creating "pragmatic networks" of stakeholders that can circumvent the barriers that often stall more formal institutional efforts and find practical solutions.[120] With greater clarity on absolute boundaries of self-help, the potential tensions from asymmetries in states' approaches can at least be contained.

Second, private sector buy-in will be crucial to establish and enforce rules of the road. The ICoC and Voluntary Principles offer models of CSR initiatives that created intrinsic incentives within the private sector to exercise certain precautions and moderate behavior. These initiatives addressed the supply and demand sides of the equation, respectively. Both are essential to incentivize realistic and effective standards for minimizing cumulative risk exposure.

Third, flexibility and adaptability are needed to keep up with the rapid evolution of technology, threats, and security practices. Self-regulation (like SAMI) and insurance proved more effective at governing behavior amid the shifting maritime security landscape and helped ameliorate the deficiencies of national regulation. As experience with self-help in cyberspace accumulates, insurance and industry associations can adapt their approaches. Moreover, these mechanisms are better-suited to address the varying circumstances across the range of private sector actors in cyberspace. Entities occupying different positions within the ICT ecosystem have different opportunities to ensure their own and others' security. The boundaries of permissible behavior should not be rigidly set nor uniform across the private sector.

Toward a Holistic Framework for Self-Help in Cyberspace

The individual insights from these analogies are merely pieces to a larger puzzle. The aim of this paper is to suggest where and how they might fit into a broader framework that starts with the gradation of policy approaches and focuses on the interacting forces shaping this space. The proper upper and lower boundaries of self-help should not be treated as unrelated policy questions.

Action in one area will have inevitable ripple effects in others due to the interdependence of cyberspace and the unique extent to which the private sector can inadvertently (or deliberately) channel risk. Allowing private actors to engage in aggressive self-help in the absence of incentives to undertake basic cybersecurity could motivate corporations to adopt an aggressive posture rather than a more cautious approach to risk minimization. However, creating space for properly circumscribed self-help that can more effectively contend with cyber threats and assist law enforcement could forestall corporations' resort to more aggressive measures—or a situation in which states are forced to intervene dramatically on behalf of the private sector.

There is a need to consider, carefully, how any policy option impacts the broader space of private self-help activity. Fully elaborating a framework for governing self-help is beyond the present scope. However, there are four broad directions for a holistic approach to circumscribing and governing self-help:

Solidify absolute boundaries of assertive self-help behavior. This should include, at a minimum, prohibiting measures or activities that pose a direct and significant risk to human safety (comparable to the hard limits on lethal defenses in the physical world). Most obviously, this includes destructive forms of hacking back. Preventing behavior detrimental to human safety can serve as a starting point for convergence upon international norms for activities exclusively in the domain of state actors.

This assertion may not be controversial. But the more counterintuitive finding of this study is that the objective of ruling out inordinately risky practices may be better served by creating space for legitimate self-help within those limits. As seen in the experience with PMSCs, building a firewall between activities that could be effectively managed and those widely considered illegitimate appears more promising—and likely more desirable—than attempting to prohibit assertive self-help altogether.

It is worth exploring, then, the various mechanisms by which states can exercise oversight while restricting the space for action: Selective forms of authorization could define narrow circumstances for defensive activities like letters of marque or—as have already been applied to cyber measures—ex

parte temporary restraining orders. Private actors could also be deputized directly by states for certain defensive functions.

Raise the bar for basic cybersecurity practices. To be clear, the focus of this study on more assertive manifestations of self-help is not to suggest these should be a first resort or that their employment would be more effective than efforts to improve basic cybersecurity and risk management, which have been thoroughly examined elsewhere.[121] A higher baseline for standard cybersecurity practices in the private sector would in many cases obviate the need to resort to more assertive defenses. So, too, would systematic efforts by corporations to preclude cyber attacks in the first place by ensuring the secure development of products and promoting an appropriately cautious approach to building new features and adding to the complexity of systems. Further, minimizing the consequences of successful attacks through systemic risk-channeling mechanisms would ameliorate the pressure on the private sector and government.

It is imperative to begin raising baseline expectations for cyber risk management through governmental and market mechanisms alike. Greater leeway for private actors to engage in more assertive forms of self-help should go hand-in-hand with clearer expectations for minimal risk management practices. Toward this end, subjecting certain entities to stricter liability for overlooking basic cyber risk management in the development and provision of products and services—appropriately defined—can effectively motivate stakeholders capable of dramatically shaping the risk landscape.[122]

Clear the way for self-help activities that would be broadly beneficial and relatively low risk. This includes those low-risk measures that have significant potential to improve defense or assist law enforcement, and that are less like force in the physical world. Some, like honeypots, are already relatively uncontroversial. These could be encouraged and supported directly by the government through efforts to build capacity and develop capabilities. Others, like digital beacons or dye packs, would benefit from greater clarity with respect to their legality (at least in places, like the United States, where there is some ambiguity). Basic technical safeguards could be required for such measures, as in the case of measures akin to anti-theft devices.

Compared to more aggressive defenses, these forms of self-help could have significant positive externalities. Simply raising the possibility that a defender will employ more sophisticated, unpredictable defenses or attribution measures creates uncertainty regarding the risks and payoffs of malicious activity. This deterrent effect would extend even to private actors that are not employing these measures.

Create the conditions for responsible conduct for those activities that can be tolerated. Certain measures, like white-hat ransomware, occupy the ambiguous space between those that are relatively innocuous and those that would be unequivocally detrimental. Clearly the private sector should not be given carte blanche to employ such measures with significant potential to cause disruption to third party networks. At the same time, it seems reasonable to conclude—based on both historical precedent and the unique considerations of cyberspace—that these measures could be justified and beneficial in certain circumstances, such as in the defense of critical infrastructure by professional cybersecurity providers.

It is therefore worth exploring how to define such circumstances through the full range of mechanisms available. Barriers to entry in the form of contractual-based authorization, licensing, or certification can limit engagement to qualified defenders. Carefully stipulated technical limitations can ensure the proportionality and reversibility of effects. Such safeguards could potentially be incorporated into certification or training requirements for operators or capabilities. Following the logic of citizen's arrest, specific circumstances such as an imminent threat to human safety could serve to authorize measures that would otherwise be off the table. Liability for the negative impacts of excessive behavior would induce further caution.

The cyber insurance industry could drive industry standards and take on a far more substantial role as a transnational proxy regulator, similar to the role it has played historically in other domains, including maritime risk.[123] The combination of liability and requirements for insurance coverage can empower insurers to enforce standards of responsible conduct, including the necessary precautions and steps for risk minimization prior to any engagement in defensive activity. Insurance can create de facto barriers to entry that would limit the space of engagement to qualified actors.

CSR initiatives can further contribute to the establishment and enforcement of industry standards. Together with insurers, industry norms and standards can condition engagement in more assertive forms of self-help upon taking all measures short of them to minimize risk exposure, including basic cyber hygiene and passive defenses. This would incentivize private actors to minimize cumulative risk exposure—not simply channel risks outward—and immediately narrow the range of cyber attacks that would justify a more assertive response.[124] Governments can empower the insurance industry to undertake this role. There have already been calls for governments to backstop insurers by underwriting catastrophic cyber risk in the same manner as is done with terrorism risk.[125]

These complementary mechanisms for incentivizing responsible conduct can begin to carve out space in which even some of the more controversial measures might become feasible. Of course, the underlying question of which measures fit into this category of potentially viable self-help activities

needs further study. But precedents from the physical world suggest it is worth considering measures like white-hat ransomware or poisoning the RAT. A blanket approach to such practices would be inordinately risky. But in the context of a holistic approach beginning with clear upper limits on behavior, an elevated baseline level of cybersecurity, and available low-risk, effective practices that can alleviate the demand for defense, it becomes realistic to consider a limited space for these practices in the toolkit of qualified defenders.

Next Steps

There is no clear end in sight to the current volatility of the cyber domain. A deteriorating cybersecurity landscape leaves the status quo increasingly untenable, yet any effort to improve upon it presents a range of dilemmas. These dilemmas reflect the underlying, fundamental struggle to reach a stable and sustainable balance between the roles and responsibilities of governments and private actors in the management of cyber risk. However, this struggle is not unique to cyberspace. It is recurrent throughout past experiences with evolving technology and new domains of human activity. Such experiences offer important insights and point to potential solutions.

Some role for self-help in a broader solution to the cyber risk challenge seems both necessary and inevitable, particularly in light of historical experience. Risk is necessary for innovation, and it would be undesirable to create an overly risk-averse atmosphere within the private sector. Yet the incentives for corporations to expand risk exposure must be contained by expectations and obligations to effectively manage risk. A balance must be struck that unlocks the vast potential in the private sector to more effectively manage cyber threats while ensuring the government's proper role in addressing the most severe threats, such as attacks on critical infrastructure.

This study has sought to outline the contours of a framework by which such a balance could be struck. It has generated individual and collective insights with immediate relevance to policy while identifying several clear directions for future efforts.

First, take stock of the full range of existing and potential mechanisms for incentivizing private actors in cyberspace. This study has described some of these: insurance, certification or licensing, regulation, and CSR. Follow up work should map out this incentive structure more thoroughly and consider options specific to different private sector entities (like ISPs and cloud service providers).

Second, further develop the salient distinctions that can differentiate activities across the spectrum of defensive measures. The focus of present debates has been primarily on the location of effects (that

is, whether or not the defender is going outside of their network). But there are a range of distinctions relevant to defining reasonable conduct: the impacts of measures, qualifications of the actor employing them, the circumstances justifying or authorizing a measure, and more. Of course, any definition of reasonable conduct must be informed by research and analysis of the efficacy of defensive measures to increase costs and reduce the payoff for malicious actors without creating offsetting risks of collateral damage.

Third, explore international and multistakeholder processes through which to begin fostering a consensus around what legitimate self-help in cyberspace looks like and developing mechanisms to discourage illegitimate behavior. Numerous international and private-sector-led initiatives already exist or are emerging that could provide platforms for discussion within industry on appropriate conduct. Even attempting to address these issues will not be without contention, but in the long run may prove far more desirable than leaving them to the combination of evolving threats and the demand for security services to define de facto norms in this space.

Progress toward defining the roles and responsibilities of private actors in the absence of robust data or experience poses a challenge. Policymakers face a kind of chicken-and-egg problem: It is hazardous to try to create boundaries for activities for which there is little collective experience with their practice. Yet it is impossible to cultivate experience and figure out what works without creating some space for legitimate practices. Nevertheless, with a cautious approach to opening up space for their employment, the risks involved appear to be manageable—especially in comparison to historical cases where self-help carried lethal consequences. Governments can begin to experiment with modes of self-help governance while being able to contain the scope, scale, and duration of activities and rein in behavior that becomes detrimental. Fostering an environment for responsible self-help may be necessary to head off far worse potential outcomes: an untenable security landscape for the private sector or a descent into vigilantism and lawlessness.

About the Authors

Wyatt Hoffman is a senior research analyst with the Cyber Policy Initiative and the Nuclear Policy Program at the Carnegie Endowment for International Peace.

Steven Nyikos is General Counsel for DayBlink Consulting and a nonresident research analyst with the Cyber Policy Initiative at the Carnegie Endowment for International Peace.

This work is the product of continuous feedback and support from colleagues through multiple revisions over time. We gratefully thank our colleagues in Carnegie's Cyber Policy Initiative, Ariel Levite, Tim Maurer, and George Perkovich, for their invaluable and encouraging editorial contributions. Additionally, we want to especially thank a number of colleagues for their advice, insights, and ideas received throughout the writing process, including Irv Lachow, Theodore Christakis, Cristin Goodwin, Michael Gadbaw, Chris Hart, Beth George, Joel Brenner, Scott Kannry, Michael Gadbaw, Gare Smith, Shavana Musa, and Deborah Avant.

Notes

[1] Notable among such efforts is the UK's National Cyber Security Centre. See Ian Levy, *Active Cyber Defense - One Year On*. UK National Cyber Security Centre. February 5, 2018.
[2] See Henry Gitter, "Self-Help Remedies for Software Vendors," *Santa Clara High Technology Law Journal* 9, no. 2 (1993)Note that the focus here is on self-help for the purposes of defense against malicious threats; other issues such as self-help remedies for commercial disputes are set aside.
[3] See, for instance, Jeff Stone, "Basic 'Cyber Hygiene' Will Help Industry Stay Ahead of Nation-State Hacking," *The Wall Street Journal,* December 13, 2017. https://blogs.wsj.com/cio/2017/12/13/basic-cyber-hygiene-will-help-industry-stay-ahead-of-nation-state-hacking/.
[4] Various definitions of active cyber defense have been supplied by technical and policy experts, with no consensus on the scope of measures included. For the purpose of examining the full spectrum of phenomena, we use ACD to refer broadly to the full range of technical measures and practices from internal-network defenses to "hacking back." For further detail on the spectrum of ACD see Wyatt Hoffman and Ariel E. Levite, *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?* Carnegie Endowment for International Peace, 2017. https://carnegieendowment.org/files/Cyber_Defense_INT_final_full.pdf.
[5] The Computer Fraud and Abuse Act (CFAA, 18 U.S.C. 1030) in the United States and similar laws in other countries prohibit unauthorized access of any computer or network, regardless of whether the computer is used for malicious activity. However, in many cases the specific applicability of such laws to a range of self-help measures and their practical enforcement remain vague propositions.
[6] See, for instance, the discussion of active cyber defense in: World Economic Forum. *Cyber Resilience Playbook for Public-Private Collaboration*. January 2018. http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf
[7] While often anecdotal, evidence of engagement in active cyber defense and hacking back by the private sector is growing; see, for instance, Joseph Cox, "Revenge Hacking is Hitting the Big Time." *The Daily Beast*, September 19, 2017. https://www.thedailybeast.com/inside-the-shadowy-world-of-revenge-hackers.
[8] For a discussion of this debate in the United States see Nicholas Schmidle, "The Digital Vigilantes Who Hack Back," *The New Yorker*, May 7, 2018. https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back.
[9] See for instance, Tim Starks, "Scoop: 'Hack back' bill gets version 2.0." *Politico*, May 25, 2017. https://www.politico.com/tipsheets/morning-cybersecurity/2017/05/25/scoop-hack-back-bill-gets-version-20-220506.
[10] Rita Abrahamsen and Michael C. Williams, *Security Beyond the State: Private Security in International Politics* (Cambridge: Cambridge University Press, 2011).
[11] Abrahamsen and Williams 2011, page 49.
[12] Lucas Kello. 2017. *The Virtual Weapon and International Order*. Cambridge: Cambridge University Press.
[13] Katz v. United States, 389 U.S. 347 (1967)—this case established the "reasonable expectation of privacy" guideline for Fourth Amendment purposes, yet the standard has also been used as a litmus test in tort actions for "intrusion upon seclusion," which has the requirement that such an intrusion upon an individual's privacy be "highly offensive to a reasonable man" according to the Restatement of the Law, 2nd, Torts (1977).
[14] As an interesting counterpoint, German law has historically prized a constitutional right to "informational self-determination," meaning that any recording of a person or their activities (that is, retention of information about their person) without the knowledge of the individual being recorded is illegal unless that recording serves an explicit public interest. See Schattauer, Christina and Demmel, Annette. *Video Surveillance in Public Areas – Lawful or Not?* Squire Patton Boggs: IP Tech Blog. January 4, 2017. http://www.iptechblog.com/2017/01/video-surveillance-in-public-areas-lawful-or-not/#page=1; Original German court ruling defining "Informational self-determination" available here (in German): http://sorminiserv.unibe.ch:8080/tools/ainfo.exe?Command=ShowPrintText&Name=bv065001.
[15] 277 US 438 (1928)
[16] 389 US 347 (1967)
[17] Winn, Peter A., "Katz and the Origins of the 'Reasonable Expectation of Privacy' Test," *McGeorge Law Review* 40 (2009): 1-13.
[18] *Ibid.*
[19] United States v. Maxwell, 45 MJ 406 (U.S. Armed Forces Ct. App. 1996).
[20] The lack of legal clarity surrounding the application of privacy laws engenders caution in the implementation of a range of measures for network monitoring and information gathering. See "CSIS/DOJ Active Cyber Defense Experts Roundtable" March 10, 2015. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150519_CountermeasuresDOJ.pdf.
[21] Packets are a form of data sent along an IP network, comprising control data (source and destination IP addresses and other pertinent details) and the payload (the user data or code which is distributed or applied at the end destination). Packets are typically the source of an intrusion or cyber attack. Traceroutes are a very common diagnostic tool that shows both the path a packet takes through the network as well as the time delay for transmission between each node in the network—but only for packets that originate

from the home network. Tracebacks, in contrast, attempt to determine the path and source of incoming packets and are highly useful in active cyber defense for both detection and attribution. IP protocol, however, is not 'authenticated,' meaning the source address can be 'spoofed,' or misrepresented. Traceback techniques are not foolproof or 100% certain.

[22] Gong, Chao and Kamil Sarac. *IP Traceback based on Packet Marking and Logging*. University of Texas at Dallas: Department of Computer Science. http://www.utdallas.edu/~ksarac/research/publications/ICC05.pdf.

[23] Katko v. Briney, 183 N.W.2d 657 (Iowa 1971)

[24] Restatement of Torts 2d – Defense of Property

[25] 183 N.W.2d 657 (Iowa 1971)

[26] Techopedia. *IP Address Blocking*. Accessed May 29, 2017. For an overview see Technopedia, "IP Address Blocking," https://www.techopedia.com/definition/3991/ip-address-blocking.

[27] Erik Kline, Alexander Afanasyev, and Peter Reiher. *Shield: DoS Filtering Using Traffic Deflection*. UCLA: *October* 2017. http://perso.telecom-paristech.fr/~hecker/FIST2011/Program_files/fist2011-s3-i2.pdf.

[28] "Cause in fact" is classically defined as the "but-for" test: would the injury have happened "but for" the automated technique? (also referred to as "sine qua non" causation). If the answer is no, then the automated technique is the cause in fact of the injury. "Proximate cause" is also called "legal cause"—meaning that the cause in fact must be reasonably foreseeable (that is, an objectively reasonable individual could have foreseen that the injury may happen).

[29] Restatement of Torts 2d – Defense of Property

[30] A "Honeynet" is a network of systems that is attractive to intruders and includes multiple "honeypots."

[31] Even, Loras R. *Honey Pot Systems Explained*. SANS: July 12, 2000. https://www.sans.org/security-resources/idfaq/what-is-a-honeypot/1/9.

[32] Spitzner, Lance. *Honeytokens: The Other Honeypot*. Symantec: 16 July 2003 (original). https://www.symantec.com/connect/articles/honeytokens-other-honeypot.

[33] DDoS means Distributed Denial of Service. A Denial of Service (DoS) attack is a method whereby the malicious actor attempts to overload a network or server's capabilities to the point of unavailability based on sheer volume of access requests. It is the most common cyber attack by far, and typically uses a network of compromised computers ("botnets") to create the problematic traffic, which is the Distributed Denial of Service (DDoS) method. *See* ST04-015: Understanding Denial-of-Service Attacks. United States Computer Emergency Readiness Team (US-CERT). Feb. 6, 2013. https://www.us-cert.gov/ncas/tips/ST04-015.

[34] The practice of citizen's arrest is under the common law, and not codified uniformly nationwide. An example can be found in the California Penal Code Section 837: "A private person may arrest another: 1. For a public offense committed or attempted in his presence. 2. When the person arrested has committed a felony, although not in his presence, 3. When a felony has in fact been committed, and he has reasonable cause for believing the person arrested to have committed it." http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEN&sectionNum=837.

[35] South Carolina State Law, 17-13-20: Additional circumstances when citizens may arrest; means to be used. http://www.scstatehouse.gov/code/t17c013.php.

[36] N.Y. Penal Law §35.30(4)

[37] SANS IDFAQ: What is Active Response? https://www.sans.org/security-resources/idfaq/what-is-active-response/5/8.

[38] The Hackback Debate," Steptoe Cyberblog, November 2, 2012. http://www.steptoecyberblog.com/2012/11/02/ the-hackback-debate/.

[39] "Hot Pursuit" can also mean the right of naval vessels to cross international jurisdictional boundaries while pursuing vessels that violated national law within their borders.

[40] Garner, Bryan A. (ed.) *Black's Law Dictionary: Seventh Edition*. West Group: St Paul, MN. 1999. (See page 677).

[41] Two commonly referenced devices are LoJack and ITURAN systems. Both have the same capabilities.

[42] Jeremy Laukkonen, "What is LoJack, and How Does It Work?" Lifewire, October 18, 2016. https://www.lifewire.com/what-is-lojack-534878.

[43] *United States v. McConney*, 728 F.2d 1195 (1984)

[44] Tony Lee, "Testing Your Defenses – Beaconing," Open Security Research, December 11, 2012. http://blog.opensecurityresearch.com/2012/12/testing-your-defenses-beaconing.html.

[45] For a description of white-hat ransomware, along with other measures, see Center for Cyber & Homeland Security, *Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats,* George Washington University, October 2016. https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf.

[46] Business Wire, "Global Card Fraud Losses Reach $16.31 Billion – Will Exceed $34 Billion in 2020 According to the Nilson Report." August 4, 2015. http://www.businesswire.com/news/home/20150804007054/en/Global-Card-Fraud-Losses-Reach-16.31-Billion#.VcJZlvlVhBc.

[47] 3SI Security Systems. *SecurityPac Brochure.* Accessed May 30, 2017. https://s3.amazonaws.com/cdn.3sisecurity.com/downloads/SecurityPac_Brochure_EN.pdf?mtime=1493210214.

[48] *Ibid.*
[49] *Taylor v. Taintor,* 83 U.S. 366 (1872)
[50] Katie B. Williams, "Does the Bounty-Hunting Industry Need Reform?" *The Atlantic*, July 23, 2015. http://www.theatlantic.com/politics/archive/2015/07/does-the-bounty-hunting-industry-need-reform/399224/.
[51] *Taylor v. Taintor,* 83 U.S. 366 (1872)—in *Lugar v. Edmondson*, 457 U.S. 922 (1982) it was established that constitutional restrictions in the Fourth Amendment (search and seizure requiring a warrant) and Fifth Amendment (right against self-incrimination) are in place whenever a bounty hunter receives "significant aid" from or "act(s) together" with law enforcement officers—because they become an instrument of the state, whose actions are limited by the Constitution.
[52] Gerald D. Robin, "Trial Practice: Reining in Bounty Hunters" *GPSolo Magazine*, March 2007. http://www.americanbar.org/content/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/reininginbountyhunters.html.
[53] PBUS is a members-only professional bail agent association. The details of their liability insurance plans can be found here: http://www.pbus.com/page/210/Liability-Insurance-Policies.htm.
[54] Admittedly, in the bounty hunter scenario the contract is signed with the tortfeasor (the individual who has committed a malicious act), and in the EULA analogy a contract is signed with a third party system owner. However, the act of contractually waiving rights against intrusion is valid in either case, and thus is the key takeaway from this analogy: it is possible for actors to obtain a contractual waiver of rights against intrusions committed for the purpose of defensive measures.
[55] "Microsoft Software License Terms: Security Essentials." https://support.microsoft.com/en-us/help/13752/windows-security-essentials-eula.
[56] Tim Greene, "Inside Microsoft botnet takedowns," *Network World*, Sept. 25, 2012. https://www.networkworld.com/article/2160165/security/inside-microsoft-botnet-takedowns.html.
[57] This may avoid criminal liability under the CFAA, which relies on 'unauthorized' access.
[58] In this way the Pinkerton Agency was not only a private investigator agency but also a private security agency, authorized to use force by the government agencies with which it contracted.
[59] Thomas Lonardo, Doug White, and Alan Rea, "To License or Not to License: An Examination of State Statutes Regarding Private Investigators and Digital Examiners." *The Journal of Digital Forensics, Security and Law*, 3, no. 3 (2014). (See page 76). http://ojs.jdfsl.org/index.php/jdfsl/article/view/176/100.
[60] The Gramm-Leach-Bliley Act (Pub. L. 106-102, Nov. 12, 1999); Impersonating an officer or employee of the United States is federally illegal under 18 U.S.C. § 912. The Federal Wiretap Act (18 U.S.C. § 2511) forbids recording as described.
[61] Guidelines for PIs that are regulated on the state level can be found in national industry associations like the United States Association of Professional Investigators (USAPI). http://www.usapi.org/about.asp.
[62] An example of private Investigator insurance plan details can be found here: http://www.ermunro.com/insurance/business/private-investigator-liability/.
[63] "Private Investigator Fact Sheet." Department of Consumer Affairs, Bureau of Security & Investigative Services. http://www.bsis.ca.gov/forms_pubs/pi_fact.shtml .
[64] Brownguard Security Professionals Liability Plan. See details here: http://brownyard.com/insurance-programs/security-guard-insurance/.
[65] See "Battling Botnets for Control of Computers" Microsoft Security Intelligence Report, 2010. http://download.microsoft.com/download/8/1/B/81B3A25C-95A1-4BCD-88A42D3D0406CDEF/Microsoft_Security_Intelligence_Report_volume_9_Battling_Botnets_English.pdf; Referencing "FRCP Rule 65: Injunctions and Restraining Orders." https://www.law.cornell.edu/rules/frcp/rule_65.
[66] *In re Louis Vuitton Et Fils S.A.,* 606 F.2d 1 (2d Cir. 1979).
[67] A botnet is a network of computers that have been compromised and are remotely controllable to some extent. Typically, such control is organized through an obscure online domain, where the malicious actor logs on and directs the botnet's activity. It is common to create multiple domains to control the same botnet, in case one or more are taken down. See *FTC v. Pricewert LLC et al.,* Case No. 09-2407 (N.D. Cal. Whyte J., June 2, 2009).
[68] "Battling Botnets for Control of Computers" Microsoft Security Intelligence Report, 2010. http://download.microsoft.com/download/8/1/B/81B3A25C-95A1-4BCD-88A42D3D0406CDEF/Microsoft_Security_Intelligence_Report_volume_9_Battling_Botnets_English.pdf.
[69] Janine Hiller, "Civil Cyberconflict: Microsoft, Cybercrime, and Botnets," *Santa Clara High Technology Law Journal* 31, no. 2 (2014).
[70] Hiller 2014.
[71] See, for instance, Paul Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures," *Stanford Journal of International Law* 50, no. 1 (Winter 2014): 2. Karine Bannelier and Theodore Christakis, "Cyber-Attacks Prevention-Reactions: The Role of States and Private Actors," *Les Cahiers de la Revue Défense Nationale*, 2017.

[72] Florian Egloff, "Cybersecurity and the Age of Privateering" in *Understanding Cyber Conflict: 14 Analogies*, eds. George Perkovich and Ariel E. Levite (Washington DC: Georgetown University Press, 2017).
[73] Abrahamsen and Williams 2011. 2011. *Security Beyond the State: Private Security in International Politics*. Cambridge: Cambridge University Press.
[74] Andrew Phillips, "Company Sovereigns, Private Violence and Colonialism" in *Routledge Handbook of Private Security Studies*, eds. Rita Abrahamsen and Anna Leander (New York, NY: Routledge 2016).
[75] Bryan Mabee, "Pirates, privateers and the political economy of private violence," *Global Change, Peace & Security* 21, no. 2 (2009).
[76] Phillips 2016, page 42.
[77] Abrahamsen and Williams 2011, page 11.
[78] Chris Demchak and Peter Dombrowski, "Cyber Westphalia: Asserting State Prerogatives in Cyberspace," *Georgetown Journal of International Affairs*, 2013.
[79] Martin Libicki, *Cyberspace in Peace and War* (Annapolis, MD: Naval Institute Press, 2016). (See page 21).
[80] Phillips 2016, page 44.
[81] Paul Rosenzweig, Steven P. Bucci, and David Inserra (2017) "Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense" The Heritage Foundation. http://www.heritage.org/sites/default/files/2017-05/BG3188.pdf
[82] Janice Thomson (1994). *Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe*. Princeton, NJ: Princeton University Press. (See page 22).
[83] Francis R. Stark, "The Abolition of Privateering and the Declaration of Paris" in *Studies in History, Economics and Public Law*, ed. Faculty of Political Science of Columbia University (New York, NY: Columbia University, 1897).
[84] Egloff 2017.
[85] For instance, see Dave Aitel, "Cyber Deterrence 'At Scale'," *Lawfare*, June 10, 2016. https://www.lawfareblog.com/cyber-deterrence-scale.
[86] Dave Aitel, "Cyber Deterrence 'At Scale'," *Lawfare*, June 10, 2016. https://www.lawfareblog.com/cyber-deterrence-scale.
[87] 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).
[88] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (New York, NY: Cambridge University Press, 2018); Irving Lachow, "The Private Sector Role in Offensive Cyber Operations: Benefits, Issues and Challenges," 2016. http://dx.doi.org/10.2139/ssrn.2836201.
[89] Andrew Nusca, "Hayden: 'Digital Blackwater' May be Necessary for Private Sector to Fight Cyber Threats," *ZDNet*, August 1, 2011. http://www.zdnet.com/blog/btl/hayden-digital-blackwater-may-be-necessary-for-private-sector-to-fight-cyber-threats/53639; Matt Apuzzo, "Ex-Blackwater Guards Given Long Terms for Killing Iraqis," *The New York Times*, April 13, 2015. https://www.nytimes.com/2015/04/14/us/ex-blackwater-guards-sentenced-to-prison-in-2007-killings-of-iraqi-civilians.html?smid=tw-share&_r=0#story-continues-6.
[90] For instance, see Alec Ross, "Want Job Security? Try Online Security," *Wired*, April 25, 2016, http://www.wired.co.uk/ article/job-security-cybersecurity-alec-ross.
[91] For an in-depth discussion of these factors see Deborah Avant, *The Market for Force: The Consequences of Privatizing Security* (New York, NY: Cambridge University Press, 2005); and Peter Singer, *Corporate Warriors: The Rise of the Privatized Military Industry* (Ithaca, NY: Cornell University Press, 2003).
[92] Deborah Avant, "Pragmatic Networks and Transnational Governance of Private Military and Security Services," *International Studies Quarterly* 60, no. 2 (2016).
[93] "The Montruex Document" International Committee of the Red Cross. https://www.icrc.org/eng/assets/files/other/icrc_002_0996.pdf .
[94] "Participating States of the Montreux Document" Switzerland Federal Departmnet of Foreign Affairs. https://www.eda.admin.ch/eda/en/home/foreign-policy/international-law/international-humanitarian-law/private-military-security-companies/participating-states.html.
[95] "The Montruex Document" International Committee of the Red Cross. https://www.icrc.org/eng/assets/files/other/icrc_002_0996.pdf.
[96] See Karine Bannelier and Theodore Christakis, "Cyber-Attacks Prevention-Reactions: The Role of States and Private Actors," *Les Cahiers de la Revue Défense Nationale*, 2017; United Nations General Assembly, A/70/174, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, 2015, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement.
[97] "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 .
[98] "International Code of Conduct for Private Security Service Providers – consensus on oversight mechanism" https://www.admin.ch/gov/en/start/dokumentation/medienmitteilungen.msg-id-47889.html.

[99] Scott Shackelford, "Human Rights and Cybersecurity Due Diligence: A Comparative Study," *University of Michigan Journal of Law Reform* 50, no. 4 (2017).
[100] For further discussion of how the ICoC could be applied to ACD, see Wyatt Hoffman and Ariel E. Levite, *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?* Carnegie Endowment for International Peace, 2017. https://carnegieendowment.org/files/Cyber_Defense_INT_final_full.pdf.
[101] Daphne Richemond-Barak, "Can Self-Regulation Work? Lessons from the Private Security and Military Industry," *Michigan Journal of International Law* 35, no. 4 (2014). (See page 819).
[102] Small Arms Survey, *Small Arms Survey 2011: States of Security* (New York: Cambridge University Press, 2011).
[103] Charles Clover, "Chinese private security companies go global." *Financial Times*, February 26, 2017. https://www.ft.com/content/2a1ce1c8-fa7c-11e6-9516-2d969e0d3b65.
[104] Small Arms Survey, *Small Arms Survey 2011: States of Security* (New York: Cambridge University Press, 2011).
[105] "Voluntary Principles on Security and Human Rights" http://www.voluntaryprinciples.org/.
[106] Abrahamsen and Williams 2011, page 107.
[107] David Axe, "Why the Somali Pirates Are Winning," The *Guardian*, April 9, 2009, http://www.theguardian.com/commentisfree/cifamerica/2009/apr/09/piracy-somalia-alabama-us-navy.
[108] 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.
[109] For an in-depth examination of the role of cyber insurance and how collaborative governmental and private sector efforts can unlock its full potential, see Ariel E. Levite, Scott Kannry, and Wyatt Hoffman, "Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance." Carnegie Endowment for International Peace, November 2018. http://carnegieendowment.org/2018/11/07/addressing-private-sector-cybersecurity-predicament-indispensable-role-of-insurance-pub-77622.
[110] See BIMCO, "GUARDCON: Standards Contract for the Employment of Security Guards on Vessels." https://www.bimco.org/-/media/bimco/news-and-trends/news/press-releases/2017/guardcon-explanatory-notes-v14--2017-update.ashx.
[111] 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. http://www.ppps.dcaf.ch/sites/default/files/uploads/Report_ICoC_Regulation_Private_Maritime_Security_Companies.pdf.
[112] The German experience with PMSCs offers an illustrative example. In 2011, the German government caved to pressure to allow armed guards out of necessity and subsequently implemented licensing procedures to re-establish authority over the practice. See 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.
[113] See Douglas Lichtman, "How the Law Responds to Self-Help," John M. Olin Law & Economics Working Paper No. 232, 2001. (See page 23).
[114] Niall McCarthy. "Private Security Outnumbers the Police In Most Countries Worldwide [Infographic]," *Forbes* August 31, 2017. https://www.forbes.com/sites/niallmccarthy/2017/08/31/private-security-outnumbers-the-police-in-most-countries-worldwide-infographic/#418bebae210f.
[115] Charles Clover "Chinese private security companies go global." *Financial Times*, February 26, 2017. https://www.ft.com/content/2a1ce1c8-fa7c-11e6-9516-2d969e0d3b65.
[116] See Douglas Lichtman, "How the Law Responds to Self-Help," John M. Olin Law & Economics Working Paper No. 232, 2001. (See page 23).
[117] David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (Oxon: Routledge, 2011). (See page 107); Paul Cornish, "Governing Cyberspace through Constructive Ambiguity," *Survival,* 57, no. 3 (2015).
[118] New York Cyber Task Force, *Building a Defensible Cyberspace*, Columbia School of International and Public Affairs, 2017. https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.
[119] For example, companies are already taking advantage of permissive environments in certain states to sell products or offer services that include various active defense measures. See Joseph Cox, "This UK Company Is Making It Easier for Private Companies to 'Hack Back,'" *Motherboard*, June 12, 2017. https://motherboard.vice.com/en_us/article/newd88/this-uk-company-is-making-it-easier-for-private-companies-to-hack-back.
[120] Deborah Avant, "Pragmatic Networks and Transnational Governance of Private Military and Security Services," *International Studies Quarterly* 60, no. 2 (2016).
[121] For a thorough discussion of the various widely available and scalable cyber risk management solutions that corporations can employ, see New York Cyber Task Force, *Building a Defensible Cyberspace*, Columbia School of International and Public Affairs, 2017. https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.
[122] Ian Levy, *Active Cyber Defense - One Year On*. UK National Cyber Security Centre. February 5, 2018. (See page 66).

[123] See Ariel E. Levite, Scott Kannry, and Wyatt Hoffman, "Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance." Carnegie Endowment for International Peace, November 2018. http://carnegieendowment.org/2018/11/07/addressing-private-sector-cybersecurity-predicament-indispensable-role-of-insurance-pub-77622.

[124] It is by now a common refrain that the vast majority of cyber attacks could be prevented by basic security practices and cyber hygiene. See, for instance, Anna Eshoo, "Promoting cyber hygiene," *The Hill,* Sept. 30, 2015. https://thehill.com/special-reports/data-security-october-1-2015/255565-promoting-cyber-hygiene.

[125] See, for instance, Oliver Ralph and Ralph Atkins, "Swiss Re chief urges governments to back cyber insurers." *Financial Times*, December 28, 2017. https://www.ft.com/content/0212ad0e-e72d-11e7-8b99-0191e45377ec.

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: +1 202 483 7600

CarnegieEndowment.org