How Does Cybersecurity Governance Theory Work When Everyone Is a Stakeholder?

Samantha A. Adams* , Karine e Silva, Bert-Jaap Koops, Bart van der Sloot Tilburg Institute for Law, Technology, and Society, Tilburg University, Tilburg, Netherlands * Samantha Adams was the lead author in the writing of this chapter. In late 2017, while the submission for this volume was under review, Samantha passed away after a brief period of illness. This chapter is one of the last pieces she wrote. The remaining authors dedicate this chapter to her memory, in gratitude for the privilege of having been able to collaborate with her.

7.1 Introduction

Because of a general impression that cyberattacks are becoming more frequent, better organized, costlier, and altogether more dangerous, countries increasingly consider cybersecurity as one of their top security issues.1 However, organizing responses to cybersecurity threats is no easy task. This chapter explores the role of polycentric cybersecurity governance in addressing cybersecurity threats, illustrated by efforts to mitigate the threats posed by botnet infrastructures. Botnets are collections of compromised machines remotely controlled by botmasters (or botherders). They are created through the dissemination of “bots,” pieces of advanced malicious software that exploit vulnerabilities and install system backdoors in various devices such as personal computers, mobile phones, tablets, and wearables. Once a bot backdoor is installed, a communication channel is established between the victim device and the network under the control of the botherders, thereby rendering the victim device's processing power and functionalities at the disposal of perpetrators. Botnets often remain under the radar of security tools such as firewalls and antiviruses, leaving users unaware that their devices are infected. Botmasters' power is reflected in their botnet's size, complexity, and resilience, which can be used to perform further criminal acts. Because they can be updated and rewired, botnets are a “living” cybercrime infrastructure. Recent industry reports revealed botnet infections affect 500 million computers every year, with 18 victims per second.2 While statistics vary and industry reports should be read cautiously, a consensus exists that botnets are among the most serious threats to information security. They are also lucrative, generating income via a multitude of cybercrimes, such as system interference, spam, search engine poisoning, extortion demands through Distributed Denial of Service (DDoS) attacks and ransomware, and click fraud.3 For example, GameOver Zeus (GOZ), a widely spread botnet that affected the international banking system until its takedown in 2014, caused an estimated loss of more than 100 million dollars worldwide.4 Newer types of botnets, such as the highly publicized Mirai,5 exacerbate these issues because they move beyond just computers to attack other networked devices such as routers, CCTV cameras, thermostats, and various other Internet of Things (IoT) devices. These types of botnets form a highly decentralized threat not only to national security but also to other public interests because they compromise private devices previously off the radar of botherders, thereby increasing the number and types of players impacted by their effects. Moreover, because any device connected to the internet can potentially be attacked, and many of these devices hold critical information about individuals' location and behaviors, there are new opportunities for highly customized attacks. By targeting the IoT, perpetrators enter a new realm of action, where attacks can be socially engineered and are more likely to succeed, since IoT devices are reportedly more poorly secured than other types of machines. The dynamic nature of botnets presents a continued challenge to developing effective security tools for detecting and disrupting botnets. Several European and non-European countries ratified the Council of Europe Cybercrime Convention6 and maintain significant levels of international cooperation in botnet mitigation.7 Yet, there is a shared understanding, especially regarding newer botnets

forms, that current mitigation approaches are insufficient. These approaches must be coupled with the strategic power of the IT industry (e.g. device manufacturers, internet service providers [ISPs], content providers, registrars, search engines, and security developers), which has a significant capacity to deter and respond to botnet attacks. Attacks against various IoT devices potentially further expand the scope of actors responsible for mitigating botnet attacks to include individual device users. However, effective incorporation of additional stakeholders is currently one weakness of cybersecurity in practice. We know from governance theory that coordinating between multiple stakeholders presents numerous challenges. The large number of agents makes the regulation of botnets notoriously complex; moreover, the potential stakeholders have different responsibilities to many different parties, some of which may conflict with one another. Effective coordination mechanisms are crucial for ensuring that these parties work together with confidence and trust. The case of botnets is useful for exploring whether, and to what extent, such response coordination works in practice. How does a multiple-stakeholder (polycentric) approach to governance work in complicated practical situations such as botnet mitigation? To answer this question, we first set the stage by conceptualizing "cybersecurity," then use the case of botnets to show the intricacies of cybersecurity in practice. After these descriptive sections, we introduce ideas from governance theory that are relevant to cybersecurity. In the discussion, we examine how the theory of "cybersecurity governance" applies to the regulation and practice of botnet mitigation.

7.2 Cybersecurity

We begin with a brief outline of primary concepts and related terms, because the way in which cybersecurity is conceptualized dictates the governance approaches that may be taken. "Cyberspace" refers to the "geographically unlimited, nonphysical space, in which – independent of time, distance and location – transactions take place between people, between computers and between people and computers. Characteristic of cyberspace is the impossibility to point to the precise place and time where an activity occurs or where information traffic happens to be."8 Cyberspace is not one homogenous space; rather, it is a myriad of virtual spaces, each providing a different form of digital interaction and communication. Cyberspace comprises both the technological components that constitute this space and the social aspects of activities taking place within it, making protection of the social and the technical equally important in approaches to cybersecurity governance.9 The term "security" refers to both the result and the process of taking measures to protect things, people, organizations, society, and the state.10 Security implies an emphasis on authority, confronting threats and enemies, an ability to make decisions, and the adoption of emergency measures.11 However, it actually demands coordinated actions on a broad range of issues and constitutes a particular type of politics applicable not only to military and political contexts but also to economic, environmental, and societal contexts.12 According to the Copenhagen School's theory of securitization, security is a discursive and political practice rather than a material condition or verifiable fact. The "threat-danger-fear-uncertainty discourse" is not universal, but "contextually and historically linked to shifting ontologies of uncertainty."13 The result and the process of security practices are equally important. In this sense, security can be described as the measures taken to safeguard the interests of a state or organization against threat. Hence, more generally, security as a process can be viewed as any checks and procedures intended to keep a person, place, or thing secure. Three more related terms are important to understanding cybersecurity: 1. Computer security refers to developing good programs with a limited number of (serious) bugs and systems that are difficult to penetrate by outside attackers. Cyber risk management is an evolution of classical computer security,

with an increasing incorporation of business-oriented concerns such as business continuity management.14 In that sense, cyber risk management is a synonym for cybersecurity. 2. Information security is “concerned with the protection of confidentiality, integrity, and availability of information in general, to serve the needs of the applicable information user.”15 Information security also includes information assurance, which deals with the underlying principles of assessing what information can or should be protected. Network security, in turn, is concerned with the design, implementation, and operation of networks – with the ultimate goal of achieving information security on networks within organizations, between organizations, and between organizations and users.16 3. Critical Information Infrastructure Protection (CIIP) refers to protecting the systems that are provided or operated by critical infrastructure providers (CIP). Critical infrastructures (or vital infrastructures) are the basal layer for socioeconomic welfare and include energy, telecommunication, banking, health, and water infrastructures. CIIP ensures that systems and networks through which critical infrastructure services operate are protected and resilient against information security and network security risks. Conceptually, the focus of cybersecurity has evolved from computer security to information security to CIIP; practically, this evolution has also trended toward an increasing number of competing interests. When computer scientists started using the term “cybersecurity” in the early 1990s, they highlighted not only the technical aspects of protecting hardware and software but also society's general vulnerabilities.17 Including social aspects, such as consequences for national security and the country's economic and social welfare, in the definition of cybersecurity also shifted attention from technical experts to public policy. Events such as the discovery of the nuclear-industry sabotaging Stuxnet computer worm, numerous tales of cyberespionage by foreign states, growing dependence on the “digital infrastructure,” and increasing media attention to highprofile cyberattacks and cyberleaks, all generated more awareness of possible future cyberattacks. Based on its components and the discussed related terms and concepts, we define “cybersecurity” as denoting both the process and the result of making cyberspace secure, where cyberspace refers not only to the space constituted by information, ICT, networks, and (ICT-based) infrastructures but also to the abstract space of digital, interconnected human and organizational activities. The security of cyberspace should consist of freedom from threats to the confidentiality, integrity, or availability of the computers, networks, and information that together constitute this space. Cybersecurity is the collection of proactive and reactive processes working toward this ideal.

7.3Botnets

Botnets are an ideal case for examining the relationship between theory and practice, due to their complex, dynamic, resilient infrastructures and the seriousness of the threats they pose to cybersecurity. A typical botnet is developed through a lifecycle of multiple, connected stages: conception, recruitment, interaction, marketing, execution, and success.18 Botnets start with the conception and dissemination of pieces of malware designed to install system backdoors and connect back to remote-controlling machines or other infected machines and servers. These “bots” are released in the wild internet or in a targeted network and exploit known vulnerabilities. Botnets are constructed such that, once a machine has been infected, it can serve as a new vector for spreading the same bot, creating an exponential effect of contamination. The aggregated infrastructure of compromised machines and channels form the so-called botnets, which further act as enablers for other cybercrime activity by offering perpetrators an army of devices (and their processing power) that can be triggered to launch new, powerful attacks. Botnets present in multiple forms are traditionally categorized by their communication channels. They may be centralized, hybrid, or peer-to-peer, depending on how

the infected machines communicate with one another.19 In centralized structures, all devices connect back to compromised servers controlled by botherders (command-and-control or C&C botnets). Aware of the vulnerability of the single point of control (once the command-and-control server is hit, the entire botnet goes down), botherders create peer-to-peer communications between bot machines, thereby programming the bot software to share pre-coded instructions with other infected machines and even launch an attack without further commands. In a P2P botnet, the botherder is replaced by an autonomous and self-managed malicious network, allowing botherders to hide and only occasionally intervene. Hybrid forms combine the control feature afforded by C&C botnets and the spider web nature of P2P botnets, offering a resilient botnet. Clearly, different types of botnets present different challenges to law enforcement and cybersecurity experts. Understanding the modus operandi of a botnet is crucial to cybersecurity efforts. Observing the communication structure is key to paralyzing a botnet before botherders have time to recode its operations. Because botherders also diversify the environment where bots operate and benefit from weaker elements of various information systems, mitigation efforts must also consider how infected devices have been compromised and the complexity of the layers in which information about the botnet can be found. For example, some known botnets exploit the darknet, a collection of non-indexed domains that are protected by multilayered structures, including The Onion Router (TOR).20 These botnets require an incredible amount of effort to break into the anonymized features of the TOR, while newer types of botnets, such Mirai or Brickerbot,21 move beyond computers to attack IoT networked devices. Botnet mitigation – the collection of efforts and measures taken to prevent, share information about, disrupt, and disinfect machines from botnets – requires more than just technical measures: it must also include measures targeting public policy, social awareness and training, legislation, and cybercrime economics. The European Union Agency for Network and Information Security (ENISA) identifies three specific approaches to fighting botnets: (i) preventing new infections, (ii) mitigating existing botnets, and (iii) minimizing criminal profit.22

7.3.1 Preventing New Infections

Important steps in preventing new infections include patching existing vulnerabilities and fostering a culture of security by design. Patching infections shields exposed vulnerabilities from contamination and immunizes them against new exploitation. Fixing nonzero-day exploits is paramount in thwarting many botnets whose modus operandi is already known to developers. A culture of security-by-design involves investment in awareness, capacity building, and training. Fostering a cybersecurity mindset among stakeholders requires the provision of incentives encouraging developers and manufacturers to be attentive to all security matters, even before the product/service is on the market, and the empowerment of users to protect themselves against botnet infections. A crucial element of prevention involves sharing information about victims and botherders, and sharing data about how botnets function. Given the widespread nature of botnets, establishing a functional network of information sharing is paramount. By distributing and compiling information about suspicious and detected botnet activity, the cybersecurity community can better prevent and respond to the menace. Information sharing is useful to smaller players that do not have the resources to invest in larger cybersecurity capabilities and can benefit from expert knowledge gathered worldwide.

7.3.2 Mitigating Existing Botnets

Although security specialists have developed powerful technical solutions to tackle botnets (e.g. P2P polluting, PeerShark, Sinkholing, Sybil attacks, and Crawling), the preparation, resources, and costs associated with large operations are often prohibitive when not supported by law enforcement and state authorities. Effective botnet mitigation tools can be highly invasive, cause collateral damages, and raise ethical and legal issues. For instance, interactive honeypots (intentionally weakened systems created to attract attackers) may breach privacy and data protection when communications established with servers and victimized machines are exposed. There is also a risk of entrapment, given that the honeypot is designed to attract malware. Mitigating existing botnets also includes disinfecting machines, which can be achieved either remotely or through awareness-raising campaigns aimed at diagnosis and disinfection by end users. The importance of raising awareness about botnet disinfection should not be underestimated. As demonstrated by Asghari et al., vulnerabilities can persist years after a patch becomes available and the botnet is taken down.23 By enabling an efficient regulatory framework and supporting private sector participation and innovation in this area, public authorities can fine-tune international cooperation models and law-enforcement powers to deliver important results – with the ultimate goals of preventing market failures from dictating security standards, and safeguarding individuals' fundamental rights.

7.3.3 Minimizing Criminal Profit

If botnets remain profitable, criminals will invest in circumventing security measures. Increasing the costs of botnets means enhancing prevention to the point that the effort to create and operate a botnet infrastructure is no longer financially interesting, and ensuring that, even when machines are infected, disruption is quick and effective. This requires raising the costs of committing botnet infection (by heightening prevention measures), raising the costs of sanctions (primarily by heightening detection and investigation capacities), and diminishing the profitability of botnets (by disrupting business models). However, these measures could merely generate replacement effects, encouraging criminal organizations to shift to targets in other sectors. If a given jurisdiction makes it more difficult to generate income through cybercrime, botnets may also migrate to countries where cybercrime is still profitable.24 Botnets constitute a special threat to cybersecurity because of the multiple agents involved. Any attempt to mitigate botnets must target and stop at least one phase of the aforementioned botnet lifecycle; hindering the completion of any of these stages frustrates botnet success.25 Ideally, botnet mitigation starts in the recruitment or contamination phase, preventing bot malware from effectively infecting targeted machines. In practice, however, most botnet countermeasures only occur after recruitment and execution, when the botnet has often already caused significant costs to business and society. The large number of agents involved in such countermeasures makes the regulation of botnets notoriously complex, and a chain of responsibility among stakeholders is currently lacking. However, successful botnet disruptions – including the GOZ, Dridex, and Ramnit takedowns coordinated by Europol's European Cybercrime Centre (EC3) and the FBI – involved action from a number of actors and relied on the expertise and extensive resources of public and private actors. Because cybersecurity issues often involve a substantial number of players acting in a complex and international environment, many scholars have suggested that such threats cannot solely be handled by regulatory measures and should not be the exclusive domain of the state.26 Rather, multiple states, businesses, and civil society organizations should play a role in a more hybrid and shared form of governance. The shift to this more hybrid conception of governance, and its relevance to botnet disruption, is explained in the subsequent sections.

7.4 Governance Theory

The governing authority at the centralized (nation–state) level has traditionally had a monopoly on power. Governments determine not only how a state is run but also which issues constitute the public interest. In modern societies, however, nongovernmental actors play an increasing role in influencing policy outcomes, thereby changing the role of centralized government. Most especially, changing dynamics in public–private relationships and influences at the systemic (international) level put the effectiveness and legitimacy of classical policy strategies and instruments up for discussion. To expand scholarly perspectives on these changes in politics and policymaking, the term "governance" was (re-)introduced in the academic vernacular of political science and public policy. Van Asselt and Renn describe governance as "the multitude of actors and processes that lead to collective binding decisions."27 This definition acknowledges that (state) governments are not the only (and possibly not even the most important) actors in managing and organizing society and social processes.28 In modern societies, the state operates in a mutually dependent triangle with the community and the market, each with its own (self-)regulatory processes. The complex interactions and dependencies within the triangle imply that all parties are affected by the unresolved problems of one.29 The interdependent state–community–market relationship moves public policy away from the traditional hierarchical, state-centric power structure to a decentralized, network structure. To reflect this difference, in the policy arena, a distinction is often made between horizontal and vertical relations. Horizontal relations show the network of relevant public and private actors that, within a defined geographical or functional segment, play a role in steering society around a common aim; vertical relations show the hierarchical links between them, highlighting institutional relations and balances of power.30 It is important to note that at the nation–state level, the governance structure is never purely horizontal or vertical: it is a mix of central and local, hierarchical and networked, vertical and horizontal – a structure also referred to as polycentric governance.31 Public–private relations are crucial in the cyber domain, and emergent governance structures for cybersecurity are both horizontal and vertical.32 According to Tuohy, the new governance paradigm "is meant to connote the processes and instruments of governing in the context of complex organizational networks in which no one set of actors has authority to 'command and control'."33 This decentralization of authority is often thought to hinder effective governance, leading to questions regarding the difference between governance and regulation. The best explanation of this distinction is offered by Helderman et al.: "Whereas 'governance' can be used for several different institutional orders (including spontaneous coordinated action) with multiple centers or networks, regulation is more restrictedly confined to the 'sustained and focused control exercised by a public—independent—agency, over private activities that are socially valued'."34 The inclusion of socially valued activities in the definition distinguishes regulatory regimes from, for example, criminal justice systems, and the reference to sustained, focused control implies that regulation is not just about law-making. It extends to include gathering information, monitoring performance, and ensuring enforcement of established rules and standards. In other words, regulation is one way that modern states steer society, among several other possible processes that may be employed to steer behaviors. Governance scholarship shows how expanding the arena of possible actors and actions simultaneously restricts the capacity of nation–state governments to act. The interdependent state–community–market relationship is thus underpinned by tensions between public and private (state and market), as well as between center and nodes (of different corners of government).35 While governance theory has encouraged scholars to think differently about the relationship between states and societies, governance itself remains a dynamic concept. Empirical studies of governance structures and processes, with a focus on effectively addressing new challenges (including cybersecurity), point to the need for more refined and

specific concepts of governance in practice. Some authors have even suggested moving away from the typology of community–market–state, public–private distinctions, and notions such as hierarchy, as all these concepts are in a state of continuous flux.36 Moreover, changing relationships between actors indicate an increased need for actors to adapt to roles in public and private environments,37 which may lead to new types of social actors or ad hoc coalitions.38 This possibility raises three practical challenges. First, the incorporation of multiple players interacting on different levels implies multiple loci of responsibility and, as such, problems with ensuring accountability for enforcement.39 There are limits to the technical capacity of government actors to define problems and understand what needs to be done in response, as well as to their institutional capacity to act once the problem has been defined. The multicentric nature of cybersecurity, as well as the multiple agendas involved in identifying problems and creating common solutions, raises the issue of command and control. Sabel and Zeitlin argue that the combination of transnational connections and increased technological innovations has undermined the effectiveness of command and control. They offer the notion of "experimentalist" governance, defined as a recursive process of provisional goal-setting and revision based on learning from the comparison of alternative approaches to advancing control in different contexts.40 The term "experimentalist" also points to the trial-and-error nature of dealing with new challenges – and to the possibility of finding creative solutions in the process. The iterative, learning-focused approach required by current governance structures and processes is related to a second practical challenge. Issues confronting society are often ambiguous and complex, demanding a flexible response given strategic uncertainty about the exact nature of the problem and how best to approach it. This challenge has been especially highlighted in the context of "risk governance," which tries to anticipate and respond to uncertainty regarding what might happen and what the consequences will be if it does. Whereas many theories implicitly seem to assume that governance is reactive, theories of risk governance and uncertainty-induced anticipation show that governance structures and strategies must also often be proactive; it is here that the lack of a single command-and-control authority, one who can or will coordinate such proactive governance, becomes problematic. The nature of many risks requires cooperation, coordination, trust, and mutual understanding among a range of stakeholders. Because these stakeholders often have both diverging interests and contrasting perceptions of potential risks involved, the various actors (including governments) tend to have difficulty making decisions with confidence and legitimacy.41 Moreover, these actors must not only minimize risk but also establish resilient systems that decrease general vulnerability to unanticipated events over a longer term. Like experimentalist governance, dealing with perceived risks often requires trial-and-error learning and seeking creative solutions. Translated to the case of cybersecurity, minimizing risks to systems and establishing longer-term systemic resilience are a challenge. Inherent to risk governance is the difficulty in pinpointing the source of (and, thus, the concrete solution to) a problem. Responses to threats are often demanded in situations where a clear analysis of the actual problem is lacking, which can lead to alarmism and overinflated threats.42 Finally, the legitimacy issues that accompany the introduction of new actors, action under uncertainty, and creative solutions (or nonsolutions) have also led to an increased demand for reflection on adopted and enacted policies and strategies. Corbridge et al. highlight the importance of attending not just to notions of governance, but to good governance43 (in accordance with social understandings of what constitutes "right and wrong"), and to how these policies and strategies can be assessed. Although agendas of good governance – and the very idea of good governance itself – may be open to critique, the primary concern from a practical perspective is ensuring the balance between individual representation and the various actors involved in governing specific cybersecurity challenges.

7.5 Discussion: Governance Theory Applied to Botnet Mitigation

Although much of the effort to fortify cybersecurity seems to be premised on increasing the criminalization of threats to – or occurring through – networked technologies,44 governance is not only about commandand-control regulation to reduce "bad" behavior. Rather, it is about the coordination of various parties in anticipation of (and in response to) potential threats – as well as the simultaneous development and implementation of longer-term structures and processes that reduce ambiguity, uncertainty, and threats from unanticipated events. Governance therefore refers to both proactive and reactive approaches to social steering, which strike a balance between stakeholder interests and the overall steering of social processes in a politically legitimate manner (i.e. in a manner that has legitimacy in the eyes of individual citizens). Initiatives led by the ITU (IMPACT),45 EU (ENISA CSIRT Network),46 and private-sector organizations in the United States (M3AAWG)47 exemplify the expansion of coordinating efforts targeted at streamlining cybersecurity practices across countries and industries. By running drills, sharing information feeds, and promoting professional training, cybersecurity initiatives have disseminated and fostered cybersecurity expertise with significant results. Yet, the world of cybersecurity information is still polarized; cybersecurity cooperation is negatively affected by the digital divide, specific industry interests, and uneven levels of political commitment. Bridging the expertise gap among consolidated and developing digital societies remains a challenge. As a deeper look into ITU-IMPACT reveals, UN assistance is much needed by countries in developing digital societies. The UN has played a strong diplomatic role in bringing together countries with conflicting political views and social systems, whereas consolidated Western digital societies have been more involved in collaborating with one another. The Joint Cybercrime Action Taskforce (J-CAT), led by the FBI and EUROPOL, symbolizes the fragmented landscape of cybersecurity cooperation among advanced economies, which arguably resembles the geopolitical alliances observed off-line. Due to the increasing dependence of most Western societies on all sorts of digital applications, such as software-based control systems, current discussions about cybersecurity focus on the vulnerabilities of critical infrastructures, transnational interdependence, and system preparedness to deal with concrete threats.48 Additionally, many Western states are paying more attention to other states as potential cyber-"enemies," resulting in the notion of cyberespionage (high-level penetrations of government and business computer systems), as well as to the "cross-fertilization" between cyberthreats and terrorism, where cyberthreats reinforce the danger posed by terrorists, and the terrorist nature of the cyberattacks makes them more attention-worthy.49 Botnets exemplify the distributed, international nature of cybersecurity threats. Deterring botnets worldwide and preventing the creation of cybercrime havens requires international cooperation and coordination. A 2015 comparative "quick scan" of cybersecurity governance in five countries – Canada, Estonia, Germany, the Netherlands, and the United Kingdom – found that botnet mitigation is largely undiscussed in national cybersecurity strategy documents, and that private actors, whose cooperation is essential, have only limited legitimate grounds for countermeasures against botnets.50 Nonetheless, the absence of a broader regulatory debate on botnet mitigation has not impeded collaboration between Europe and North America in combatting ubiquitous botnet infections, as the case of GOZ shows. GOZ was a widely spread botnet affecting financial transactions operated by the so-called "Business Club," a criminal ring allegedly headed by Evgeniy Mikhailovich Bogachev. Aside from capturing victims' bank data and credentials, GOZ operated as the main channel for disseminating Cryptolocker, a form of ransomware (a variety of malware that blackmails users while requesting a ransom). In the complaint directed to the US District Court of Western Pennsylvania, as part of the legal procedure that led to the takedown of GOZ in mid-2014, the US government claimed the combined losses caused by GOZ and

Cryptolocker exceeded 100 million dollars and infected thousands of machines worldwide.51 On 3 June 2014, the District Court granted the US government request to a takedown of the infrastructure of both GOZ and Cryptolocker, takeover of the Cryptolocker DGA domains, and takeover of the peer-to-peer network of GOZ.52 However, the efforts leading to the worldwide and almost simultaneous GOZ takedown were part of a broader international law-enforcement collaboration not limited to the US Operation Tovar, steered by the FBI and Europol (EC3), pooled the resources of public and private sector organizations across jurisdictions. It was built upon the findings of law-enforcement agents from Canada, Japan, Ukraine, and New Zealand, as well as EU Member States (including Germany and the Netherlands) and the United States, but also counted on support from private-sector partners, including Dell SecureWorks, Microsoft Corporation, McAfee, Symantec, Abuse.ch, Afilias, Crowdstrike, Delloite, F-Secure, Georgia Tech, Heimdal Security, Level 3 Communications, Neustar, Sophos, Trend Micro, and nonprofit organizations such as Shadowserver and Carnegie Mellon.53 Further details on how law enforcement, industry partners, and academic and civil society organizations from various countries collaborated to take down GOZ were not made available to the public – presumably, these files have been sealed by national authorities, as disclosure about the means and methods of investigation may compromise future endeavors. Yet, it is possible to infer that the actions undertaken during the operation and the resulting outcomes necessitated the exchange of substantial amounts of evidence concerning victims and perpetrators, including information about the mitigation techniques applied to gather data and disrupt GOZ. The secrecy applied to such high-level anti-botnet efforts has the drawback of paralyzing public scrutiny and oversight of the ways in which privacy of communications and individuals – including both information privacy and data protection – was respected throughout the investigation. While confidentiality of otherwise public procedures may be granted by the circumstances of the case, the degree and nature of participation by private-sector agents was overshadowed by reports focused on highlighting the promising results of PPPs and the social contribution of the private sector to the greater public interest. Public access to information was similarly restricted in the case of Dridex, a variation of GOZ. Dridex emerged shortly after the GOZ takedown, which clearly had not stopped its commanders from launching another devastating botnet. Although Dridex was the most prevalent Trojan online in 2013,54 its activity period was much shorter. It was taken down in late 2015 through a collective effort, claimed to be led by the FBI55 and involving the US-CERT, the UK National Crime Agency, Europol (EC3), German Bundeskriminalamt (BKA), Dell SecureWorks, Fox-IT, S21 sec, Abuse.ch, the Shadowserver Foundation, Spamhaus, and a Moldovan cybercrime police agency. However, access to information about the workings within the consortium remains restricted. Although the mechanics of such supranational, public–private efforts remain somewhat obscure, they clearly are – to some extent – successful. This success is partly owed to two important elements, shared by the countries studied in the comparative quick scan: supranational legislation and national-level Computer Emergency Response Teams (CERTs). In a prime example of supranational legislation, all five countries had ratified the Cybercrime Convention, the first international treaty to address internet- and computer-related crimes. The Convention sought to approximate national laws and increase cooperation between countries, but it actually acts as a minimum catalog of offenses and investigation powers, leaving room for countries to implement its principles within their own legal cultures. Even among the five countries, there were significant differences in both criminal law and investigatory powers that made this arrangement ideal. These differences usually related to differences between civil law and common law traditions. Civil law countries, for example, more strongly emphasized the statutory limits to invasive investigative measures. Nevertheless, the Convention also enhances possibilities for international cooperation, through harmonized minimum levels of

criminalization (ensuring the legal requirement of double criminality does not hamper mutual legal assistance), its investigation powers (increasing the likelihood of evidence acquisition), and its provisions for mutual assistance and a 24/7 contact-point network. Therefore, despite national variations in legal approaches to botnet mitigation, supranational law is an important facilitator in fighting botnets: ratification of the Cybercrime Convention provided a shared basis for international cooperative efforts against botnets. When coordinated action was necessary to take down a botnet, the command-and-control function of the government and police became evident. Each of the five countries also has its own national-level CERT. These CERTs have the mandate to oversee threats on their national territory, and the procedures they follow are largely harmonized. CERTs distribute relevant information within circles of trust. Since such information is often undisclosed to a larger audience, it is not possible to evaluate the impact and the influence of national CERTs countering botnets, beyond what is made publicly available online. However, all five countries have participated in international cooperative efforts against botnets. Many of these international cooperation activities revealed a connection with Europol's (EC3) and the US FBI's efforts in fighting botnets, demonstrating the important role played by both institutions in coordinating international cooperation. To some extent, then, this disproves the theoretical view that polycentric governance lacks coordination capacity: supranational and important national state-based actors clearly can take up coordination responsibility in cybersecurity governance practice. Botnets, especially those that target IoT devices, exemplify the convergence between three levels of cybersecurity: the macro-level, focused on protecting critical infrastructures at the nation–state level; the meso-level, focused on protecting manufacturers, service providers, and the like; and the micro-level, focused on protecting every day, ubiquitous networked personal devices. In the age of IoT and ubiquitous connectivity, the number and types of players involved with or possibly instrumental in fighting botnets has significantly increased. Because millions of infected IoT devices collectively can be used to attack various types of infrastructures, responsibility for mitigation of botnet attacks rests not only with formal authorities but also with manufacturers, service providers, and even individual citizens. But these different players have different responsibilities to many different parties, which may come into conflict with one another. For example, ISPs have an opportunity to take preventive measures; in addition, they can be instrumental in blocking and/or tracing the sources of botnet attacks. They are also often in a good position to collect information about attackers and infected machines from a pragmatic point of view. However, it is not always clear how far ISPs can go, both legally and morally, in cooperating with public authorities – especially law enforcement – in the context of mitigation. Arguments in favor of greater ISP participation in botnet mitigation frequently emphasize their technical expertise and strategic role in managing the exchange of information among targets, compromised machines, malicious servers, and botherders. The speed with which ISPs can identify, halt, and divert attacks clearly far surpasses that of law-enforcement remedies. In addition, ISPs arguably do share a responsibility to keep the internet safe, as they are interested in both securing their reputation before customers and protecting their networks from malicious interference. Yet, advocates of ISP involvement often overlook the fact that ISPs – although they are ideally positioned to preempt, respond, and thwart botnet attacks – may lack the legitimacy to make pivotal decisions about cybercrime offenses. First, there is a prominent and ongoing debate about the legitimate role ISPs can play in delivering cybersecurity. Traditionally, matters of public security – such as guaranteeing the security and integrity of information systems and their users – are solely the task of the state; it is for public institutions and delegated agencies to define cybersecurity and crime-fighting policies. Shifting social expectations of cybersecurity, at least partly, to the hands of ISPs, does create a risk of democratic deficit: ISPs are not bound by the high standards of transparency and accountability to which public agents are subject. Ultimately, transferring

the task of cybersecurity from the public to the private sector, without the safeguard of public accountability, may compromise the state's role as the primary guarantor of the rule of law. Second, increasing ISP involvement in cybersecurity may result in higher risks to information privacy. Without a proper system of accountability recalibrated to respond to the significance of ISP intervention in cybersecurity, there is a risk that information that would otherwise be collected through law-enforcement procedures – which, in general, are subject to judicial oversight and other checks and balances to minimize the impact of privacy interferences – would be amassed under lower thresholds. The absence of societal and institutional control over the collection, analysis, and distribution of information relevant to botnet mitigation – which often involves examining large sets of data pertaining to the personal identity, online behavior, and location of users – could culminate in serious privacy violations. Altogether, intensifying the participation of ISPs in botnet mitigation would necessitate revisiting the rules applicable to service providers online. This option would have to lead to higher thresholds of accountability and transparency regarding how ISPs process information, and clear liability rules implicating ISPs for potential misuse of this newly invested power. As a result of the unresolved regulatory debate concerning the responsibilities of ISPs in cybersecurity, the types of action that ISPs can legally take are still limited. Attempts to formalize an increased role for ISPs remain limited to changing their Terms of Use to broaden the scope of the actions they can take. Such considerations are also applicable to other players involved in the spread or prevention of botnets, including cloud computing providers, software developers, hardware manufacturers, and search engines. States can resume an authoritative position in cybersecurity by taking and stimulating both preventive and reactive measures. Preventive measures include providing more incentives for organizations to patch known vulnerabilities, ensuring greater control over the use of zero-day vulnerabilities (hotly debated in Dutch public policy in the context of police hacking)56 and stimulating information sharing concerning intelligence data on botnets. Reactive measures include, for instance, redirecting compromised devices to safe servers and patching vulnerabilities. It is now understood that the spread of Mirai was largely due to precarious security choices made at the manufacturing level, including the use of default usernames and passwords to protect the stream of devices placed on the market.57 Once the credential vulnerabilities were discovered by cybercriminals, brute-forcing the predictable range of hardcoded keys was an easy way to acquire control over a massive number of IoT devices. Although fixing the exploit should have been as simple as alerting users about the need to reset the default passwords and usernames, the fact that the system credentials were hardcoded into the devices made it possible for criminals to access the system panels through additional communication channels even after the reset.58 The Mirai case exemplifies the need to internalize security from inception to manufacturing (security-by-design), but also the failure of states to ensure that basic cybersecurity standards are respected throughout the industry. Because citizens are generally unaware of the fact that they (or more precisely, their devices) are instrumental to such attacks, states can also increase awareness through public information and education programs on the importance of personal device security. 7.6 Conclusion Cybersecurity governance refers to various approaches used by stakeholders to identify, frame, and coordinate both proactive and reactive responses to threats to the technical and social layers of information infrastructures. Over the past few years, political actors at the national level – including federal agencies, police authorities, and key interest groups – have produced policy documents that highlight the need to protect information infrastructures; increasingly, these documents also specify what constitutes a given infrastructure, the nature of possible threats to that infrastructure, and the social sectors that will feel the effects of those threats. At the same time, such documents reveal the high degree of polycentric governance within and between countries, which can lead to confusion regarding who is responsible in the case of a

major incident. Increasingly, states seem to recognize that the nature of the problem is so large that it is insufficient to designate one lead agency to manage it. In many countries, various parties are even being encouraged to develop their own CERTs (in addition to those already established at the national level). Given the increasing multitude of players interacting in the cybersecurity landscape, cooperation and coordination isare necessary to prevent threats to this infrastructure and its component parts, as well as to deal with incidents when they occur. The cross-border efforts to take down large-scale botnets, led by the FBI and Europol, exemplify the ways in which law enforcement and private-sector parties are engaged in combatting ubiquitous cybercrime. In the field of cybercrime, the actions of J-CAT have become the new rule – and the model through which transnational criminal justice is pursued against cybercrime. Cybersecurity governance includes not only short-term and concrete approaches to address known threats but also the development and implementation of structures and processes to reduce uncertainty and enable responses to threats from unanticipated events over the longer term. Botnet mitigation efforts show the contours of such cybersecurity governance in practice, demonstrating that polycentric governance can work effectively if some (typically supranational or based around a key nation) actors take up responsibility for coordinating efforts, and if basic legislative frameworks are in place to facilitate international cooperation. Nevertheless, botnet mitigation efforts until now have often been more reactive than proactive, and focused on the short term rather than the long term, suggesting that risk governance is a daunting task far easier conceptualized than enacted.

Notes

1Myriam Dunn Cavelty, "The Militarisation of Cyber Security as a Source of Global Tension," in Strategic Trends and Analysis: Key Developments in Global Affairs, ed. Daniel Möckli (Zurich: Center for Security Studies, 2012), accessed November 9, 2017, http://www.css.ethz.ch/publications/pdfs/StrategicTrends-2012-Cyber.pdf. 2 Joseph Demarest, "Taking Down Botnets," Testimony Before the United States Senate Judiciary Committee, Subcommittee on Crime and Terrorism, July 15, 2014, accessed November 9, 2017, http://www.fbi.gov/news/ testimony/taking-down-botnets. 3Alvaro A. Cardenes et al., "An Economic Map of Cybercrime," Working Paper 2009, accessed November 9, 2017, http://chess.eecs.berkeley.edu/pubs/772/cardenas_2009.pdf. 4United States Federal Bureau of Investigation (FBI), "GameOver Zeus Botnet Disrupted Collaborative Effort Among International Partners," June 2, 2014, accessed November 9, 2017, https://www.fbi.gov/news/stories/ gameover-zeus-botnet-disrupted. 5Brian Krebs, " Who Makes the IoT Things Under Attack?" Krebs on Security Blog, October 3, 2016, accessed November 9, 2017, https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack. 6Convention on Cybercrime, Budapest, 2001, CETS 185. 7 Samantha Adams et al., The Governance of Cybersecurity. A Comparative Quick Scan of Approaches in Canada, Estonia, Germany, The Netherlands and the UK (Tilburg/The Hague: TILT/WODC, 2015), accessed November 9, 2017, https://www.wodc.nl/binaries/2484-volledige-tekst_tcm28-73672.pdf. 8Cees J. Hamelink, The Ethics of Cyberspace (Thousand Oaks, CA: Sage, 2001), 9. 9 Jan van den Berg et al., "On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education," paper presented at the NATO STO/IST-122 Symposium, Tallinn, October 13–14, 2014, 12-2. 10"Security," Oxford English Dictionary, accessed November 9, 2017, www.oed.com. 11Lene Hansen and Helen Nissenbaum, " Digital Disaster, Cyber Security and the Copenhagen School," International Studies Quarterly 53 (2009), 1155–1175. 12Barry Buzan et al., Security: A New Framework for Analysis (London: Lynne Riener, 1998), vii, 1. 13Niels Bubandt, " Vernacular Security: The Politics of Feeling Safe in Global, National and Local Worlds," Security Dialog 36 (2005): 291, as cited in

Hansen and Nissenbaum “Digital Disaster,” 1172. 14Van den Berg et al., “On (the Emergence of) Cyber Security Science,” 12-2–12-3. 15Alexander Klimburg, National Cybersecurity Framework Manual (Tallinn, Estonia: NATO, 2012). 16Ibid. 17Hansen and Nissenbaum, “Digital Disaster”; Dunn Cavelty, “Militarisation of Cyber Security.” 18Rafael A. Rodriguez-Gomez et al., “ Survey and Taxonomy of Botnet Research Through Life-Cycle,” ACM Computing Surveys 45 (2013). 19Ahmad Karim et al., “ Botnet Detection Techniques: Review, Future Trends, and Issues,” Journal Zhejiang University-SCIENCE C (Computers & Electronics) 15 (2014): 948. 20Marie-Helen Maras, “ Inside Darknet: The Takedown of Silk Road,” Criminal Justice Matters 98 (2014): 22. 21Trendmicro, “BrickerBot Malware Emerges, Permanently Bricks IoT Devices,” April 19, 2017, accessed November 9, 2017, https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/brickerbotmalware-permanently-bricks-iot-devices. 22Jan Gassen et al., “Botnets: How to Fight the Ever-Growing Threat on a Technical Level,” in Botnets, ed. Heli Tiirmaa-Klaar et al. (London: Springer, 2013). 23Hadi Asghari et al., “Post-Mortem of a Zombie: Conficker Cleanup After Six Years,” Proceedings of the 24th USENIX Security Symposium, 2015, accessed November 9, 2017, https://www.usenix.org/system/files/ conference/usenixsecurity15/sec15-paper-asghari.pdf. 24Nir Kshetri, The Global Cybercrime Industry (London: Springer, 2010), 48. 25Rodriguez-Gomez et al., “Survey and Taxonomy.” 26Myriam Dunn Cavelty and Manuel Suter, “ Public-Private Partnerships are no Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection,” International Journal of Critical Infrastructure Protection 2 (2009): 179–187; Judith H. Germano, Cybersecurity Partnerships (New York: Center on Law and Security, New York University, 2014). 27Marjolein van Asselt and Ortwin Renn, “ Risk Governance,” Journal of Risk Research 14 (2011): 431. 28Ibid. 29Wolfgang Streeck and Philippe Schmitter, “ Community, Market, State-and Associations? The Prospective Contribution of Interest Governance to Social Order,” European Sociological Review 1 (1985): 119. 30See Van Asselt and Renn, “Risk Governance,” 434; Broeders, Investigating the Place and Role, 12. 31Eelco Van Hout et al., “Governance of Local Care and Public Service Provision,” paper presented at the EGPA Conference, Madrid, September 19–22, 2007. 32Broeders, Investigating the Place and Role, 16, 44. 33Carolyn H. Tuohy, “ Agency, Contract and Governance: Shifting Shapes of Accountability in the Health Care Arena,” Journal of Health Politics, Policy and Law 28 (2003): 202. 34Jan-Kees Helderman et al., “ The Rise of the Regulatory State in Healthcare: A Comparative Analysis of the Netherlands, England and Italy,” Health Economics, Policy and Law 7 (2012): 105. The authors quote Majone 1994 in the second half of the definition. 35Robert H. Blank and Viola Burau, Comparative Health Policy, 3rd ed. (Houndmills: Palgrave Macmillan, 2010), 69. 36See, for example,Taco Brandsen et al., “ Griffins or Chameleons? Hybridity as a Permanent and Inevitable Characteristic of the Third Sector,” International Journal of Public Administration 28 (2005), 749–765; Tim Tenbensel, “ Multiple Modes of Governance,” Public Management Review 7 (2005). 37Van Hout et al., “Governance of Local Care.” 38Van Asselt and Renn, “Risk Governance.” 39Tuohy, “Agency, Contract and Governance.” 40Charles F. Sabel and Jonathan Zeitlin, “Experimentalist Governance,” in The Oxford Handbook of Governance, ed. David Levi-Faur (Oxford: Oxford University Press, 2012). 41Van Asselt and Renn, “Risk Governance.” 42Broeders, Investigating the Place and Role, 7–11. 43Corbridge, S. et al., Seeing the State (Cambridge: Cambridge University Press, 2005), 152. 44Cf.Bert-Jaap Koops, “ Technology and the Crime Society: Rethinking Legal Protection,” Law, Innovation and Technology 1 (2009): 93–124. 45See Impact Alliance, “Mission & Vision,” accessed November 9, 2017, http://www.impact-alliance.org/ aboutus/mission-&-vision.html. 46See CSIRTs in Europe, “Capacity Building,” accessed November 9, 2017, https://www.enisa.europa.eu/ topics/csirts-in-europe/capacity-building. 47See M3AAWG, “About M3AAWG,” accessed November 9, 2017,

http://www.m3aawg.org/about-m3aawg. 48Ted Koppel, Lights Out (New York: Penguin, 2015). 49Dunn Cavelty, “Militarisation of Cyber Security.” 50Adams et al., Governance of Cybersecurity. 51United States of America vs. Evgeniy Mikhailovich Bogachev [2014] Civil Action No. 14-0685 (United States District Court for the Western District of Pennsylvania). 52Ibid. 53Europol, “International Action Against ‘GameOver Zeus’ Botnet and ‘Cryptolocker’ Ransomware,” June 4, 2014, accessed November 9, 2017, https://www.europol.europa.eu/newsroom/news/international-actionagainst-gameover-zeus-botnet-and-cryptolocker-ransomware. 54Dick O'Brien, “Dridex: Tidal Waves of Spam Pushing Dangerous Financial Trojan” (Mountain View: Symantec, 2016), accessed November 9, 2017, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf. 55United States Federal Bureau of Investigation (FBI), “Bugat Botnet Administrator Arrested and Malware Disabled,” October 13, 2015, accessed November 9 2017, https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/bugat-botnet-administrator-arrested-and-malware-disabled. 56Kamerstukken I [Dutch Parliamentary Proceedings First Chamber] 2016/17, 34372, no. E, 39-45 and no. F, 2-4. 57Brian Krebs, “Who Makes the IoT Things Under Attack?” 58Ibid.