International Review of Law, Computers & Technology

ISSN: 1360-0869 (Print) 1364-6885 (Online) Journal homepage: https://www.tandfonline.com/loi/cirl20

How industry can help us fight against botnets: notes on regulating private-sector intervention

Karine K. e Silva

To cite this article: Karine K. e Silva (2017) How industry can help us fight against botnets: notes on regulating private-sector intervention, International Review of Law, Computers & Technology, 31:1, 105-130, DOI: 10.1080/13600869.2017.1275274

To link to this article: https://doi.org/10.1080/13600869.2017.1275274

© 2017 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

Published online: 22 Feb 2017.

Submit your article to this journal

Article views: 1798

View related articles

View Crossmark data

Citing articles: 2 View citing articles

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=cirl20

INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY, 2017
VOL. 31, NO. 1, 105–130
http://dx.doi.org/10.1080/13600869.2017.1275274

Routledge
Taylor & Francis Group

OPEN ACCESS

How industry can help us fight against botnets: notes on regulating private-sector intervention[†]

Karine K. e Silva

Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Tilburg, Netherlands

ABSTRACT

Could industry improve our response to botnet attacks? If so, how should this private-sector participation be regulated? This paper examines how regulation could be used to facilitate private-sector intervention against robot networks, also known as botnets. The first part is dedicated to exploring botnets and the potential role industry could play to mitigate them. The second part exposes the obstacles that must be addressed by regulators attempting to further industry participation in this arena. The third part outlines starting points for regulating this specific form of private-sector intervention. These starting points build upon the pioneering efforts launched in the Netherlands, US, Germany, and Finland, and present a compass for guiding regulatory choice. Stemming from these considerations, a hard law and two soft law mechanisms are presented as a commencement for regulating industry intervention. Finally, because this paper adopts an international, high-level approach, its findings may support regulatory efforts in various parts of the world, given the omnipresent challenge posed by botnets.

KEYWORDS

cyber security; cyber crime; botnets; public-private partnerships

1. Introduction

The prevalence of cyber threats has ignited a fervent discussion on the effective means to counter cybercrime. Among the proposed strategies arising from this debate, the idea of furthering Internet industry participation attracts particular attention. This study stems from the widespread belief, corroborated by governmental efforts, that the prominent position held by businesses on the operation, monitoring, and delivery of Internet services, renders private sector well positioned to preempt and counter cybercrime. Could industry help us fight against botnets? If so, could regulation facilitate this contribution? These are some of the problems explored in the following sections.

As highlighted by Brenner (2007, 61), businesses can support law enforcement agencies by providing relevant means for investigation and expert knowledge, apart from directly supporting criminal procedures by allocating staff members to collaborate with the authorities. In addition to being helpful to investigations, private-sector actors are equipped

CONTACT Karine K. e Silva K.K.ESilva@uvt.nl

[†]This study is fruit of my PhD research, funded by the NWO BotLeg project, a research consortium that brings together public and private sector fighting against botnets.

© 2017 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

with sufficient resources to timely detect, prevent, and respond to cybercrime as it occurs (Germano 2014, 2). However, given the diversity of private-sector stakeholders, it seems befitting to speak of a category of business with direct and complementary capabilities of countering cybercrime, or an Internet industry composed of Internet Service Providers (ISPs), registrars, hosting providers, and IT security companies (herein: Internet industry). From a utility lens, incorporating the combined power of the Internet industry to respond to cybercrime is a latent, yet promising step towards improved security. While public authorities hold prerogatives for investigation and prosecution of crimes, the Internet industry has expert insight into combatting cyber threats (Germano 2014, 2) and the tools to prevent and disrupt online criminality before judicialization.

In spite of the promises that nations will enhance their response to cybercrime by involving the Internet industry, opposing arguments challenge the viability and legitimacy of a hybrid model of law enforcement composed of shared responsibilities between public sector (in charge of criminal investigations) and private companies (capable of preventing and disrupting attacks). The concerns about expanding private-sector participation in fighting cybercrime outside the scope of a criminal investigation are threefold: (1) States concentrate legitimacy on the use of force in the hands of law enforcement authorities, therefore excluding private sector, (2) The Internet industry is not bound to transparency and accountability in the same form as public actors, and their misconduct could be left unpunished, and (3) Regulatory incentives are arguably insufficient to ensure the Internet industry will act on public interest, whenever these contrast with their private interests.

The debate on Internet industry participation converts into a vital question when considering high-impact forms of cybercrime. Within the broadening scope of cyber threats, I chose to focus on botnets, known as the backbone of modern online criminality. The term 'Botnets' stand for networks of compromised devices infected by a 'bot' computer program, and may comprise millions of victimized devices. A bot, simply put, is an advanced piece of software designed to create malicious backdoors that allow criminals to remotely control infected systems. By manipulating this large network of devices, criminals are able to launch powerful cyber-attacks against websites, companies, and users themselves (Narang et al. 2014, 108).

The experience of 'successful' botnet takedowns, namely Gameover Zeus (FBI 2014), ZeroAccess (EUROPOL 2013), and Ramnit (EUROPOL 2015) substantiate the involvement of private sector as a prominent factor for effective botnet mitigation. Next to cooperating with public authorities, private-sector actors may collaborate with one another: they exchange data and promote disinfection of botnets together. As a result and due to the pivotal role played by the Internet industry in countering botnets, cooperation between public authorities and private parties has been at the heart of anti-botnet discussions (ENISA 2011). Owing to the fact that botnets avail themselves from the ubiquity of the Internet, whose services and infrastructures are typically operated by business intermediaries, the possibility of counting on the support of the Internet industry is paramount to preventing new attacks.

Nevertheless, Internet industry partaking in botnet mitigation is insufficiently regulated. Despite its potential, industry collaboration remains in a regulatory vacuum: businesses willing to combat botnets are at a loss as to which countermeasures are legitimate, what types of data can be exchanged with public authorities and other

third parties, and how different forms of cooperation may translate into liability. Moreover, it is not clear which actors should be involved in this effort or whether existent frameworks effectively accommodate Internet industry participation. Not all these questions can be answered here. Rather, I will attempt to offer some guiding points for regulating botnet countermeasures by private sector and a set of recommendations that may prove valuable to regulators.

2. The evolution of cybercrime

The dissemination of computer technology was accompanied by an increase in sophistication of cybercrime. As noted by Zittrain (2008, 70), the generative nature of the Internet, meaning the fact that code may be developed and distributed by anyone in the world, is the essence of the Internet, as well as its Achilles' heel. Zittrain goes on to explain that the design embodied by the Internet is a result of the constraints and beliefs of its inventors, who were mostly academics with limited resources and without a personal interest in enabling centralized control over users' activities online (Zittrain 2008, 28). For their very origin, information networks were available for dual-use by its visitors, and that meant the Internet could be used for licit and illicit purposes. Ergo, the evolution of the Internet and misuse of information systems unraveled as the opposite sides of the same coin.

Cybercrime, just as the Internet, evolved in a decentralized and global manner, together with the skills of individuals across the world experimenting with new technology. By converting these discoveries into techniques for committing crimes, a different wave of criminality was created, giving rise to the label 'cybercrime'. Fast-forward to today, cybercrime has become an elaborate means for committing crime and one of the biggest threats to our Internet-dependent society. Advanced forms of cybercrime target vulnerabilities in widespread software, massive data flows, and valuable databases, compromising not only the fruition of personal devices but also fundamental services such as transportation, electricity, and the Internet itself (and other forms of Critical Infrastructure). Presently, the most devastating face of cybercrime threatens information networks connected to the well-being of citizens, including threats to national security, critical infrastructure, and the Internet of Things (IoT).

3. Botnets: an overview

Botnets or 'roBOT NETworks' are collections of machines infected by a 'bot' and remotely controlled by a 'botmaster'. Typically, a bot infection creates backdoors that communicate back with the remote master, reporting the successful infection (Narang et al. 2014, 108). The bot installation is automatic and mostly independent from user participation. After installed, a botnet infection will integrate the compromised machine into the network of botnets, marking the moment in which the machine becomes another soldier in the bot army. The user, however, seldom spots the infection, as bot malware have been developed to conceal their operations and stay under the radar of security software. Complex forms of cybercrimes such as botnets are particularly pervasive because of their automation feature. In a botnet, the attack is commanded by the botmasters, but performed by the machines that have been captured by them.

The origin of botnets dates back to the late 1980s, when they were conceived as helpful tools that could expedite the time and effort spent on repetitive computer tasks (ENISA 2011, 13). The power to remotely control machines and execute orders from a distance, the main characteristic of a botnet, was perceived by criminals too, who saw how these functionalities could help committing online crimes. Botnets have since evolved from simple networks running on online chats to worldwide structures threatening the functioning of the digital economy. Since their first appearance in Internet chats, botnet infrastructures expanded to complex protocols and, most recently, to social media, mobile, and cloud-based networks (Clark, Warnier, and Brazer 2011). This process of diversification has made bot infections more persistent, threatening, and profitable. Finally, because botmasters often target devices regardless of their geographical location, online users share the global risks and challenges posed by botnets (Figure 1).

Owing to their scale-effect, the economic losses caused by botnets are massive. In 2013, Chameleon botnet, a piece of malware exploiting online ads, allegedly caused a 6 million dollar monthly loss to website advertisers (Spider.io 2013). A year later, the costs attributed to GameOver Zeus, a botnet intercepting online banking transactions, reportedly reached over 100 million dollars (FBI 2014).[1] Financial costs aside, botnets also account for a large social cost (Anderson et al. 2012, 6): (1) they infringe on the fundamental right to privacy in that they compromise personal, traffic, and location data of individuals; (2) they cause job losses by obstructing and compromising targeted systems victims of the attacks; and (3) they harm trust in the digital society by demonstrating how vulnerable both users and online services are. A striking destructive use of botnets has been associated with cyberwarfare and politically motivated attacks. The events that affected Estonia in 2007, compromising the availability of websites of the government, media, and two important banks for

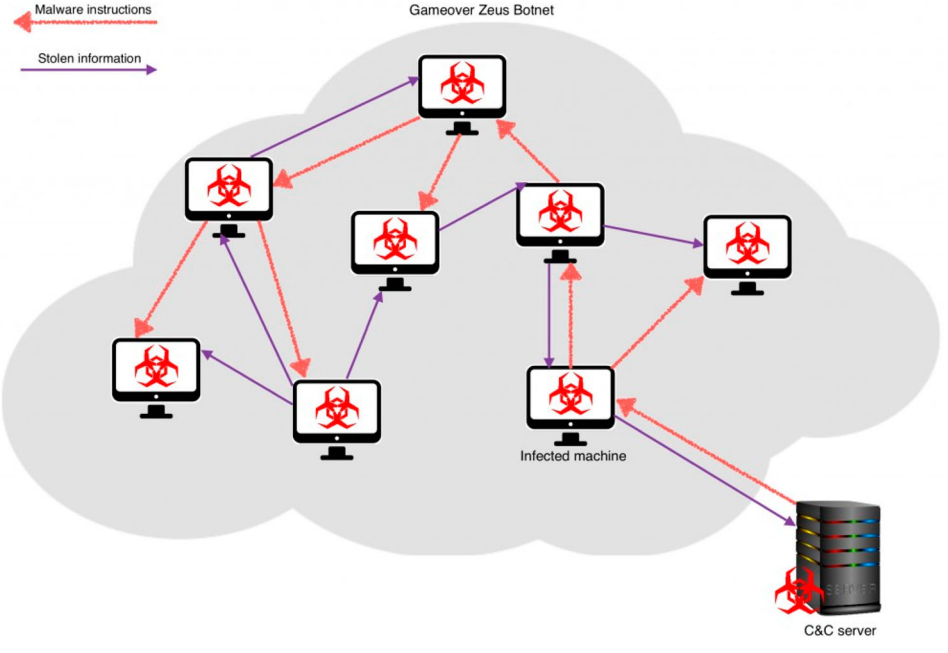

Figure 1. Gameover Zeus simplified structure: a P2P botnet architecture (O'Connell 2014).

days (Hansen and Nissenbaum 2009), are a notorious example of how botnets can be deployed to launch powerful attacks, as well as how cyber-attacks can have massive, disturbing consequences on a nation and its people.[2] The progressive vulnerability of our information society, deeply entrenched into technology, has led governments to reconsider their own role in ensuring cybersecurity and to recognize the Internet industry as the critical node for safeguarding information systems. (Tropina and Callanan 2015, 13–14).

3.1. How botnets spread

In order to gain access to a computer system and connect it to the botnet, botmasters often use infection vectors, known as a category of means that propagate contaminations from one machine to another. For botmasters, infection vectors are the preferred means for infecting machines (Tiirmaa-Klaar et al. 2013, 43), as they offer a direct interaction between the bot and the targeted device, increasing the chances of successful contamination. This aggressive approach is capable of compromising even highly secure and trusted systems (Tiirmaa-Klaar et al. 2013, 51), since infection vectors are not always dependent on manifest vulnerabilities or user interaction (McAfee 2011). The list of popular infection vectors explored in this section includes drive-by-download, Trojans, worms, email, and messaging.

Drive-by-download represent the automatic delivery of malicious HTML documents inserted in compromised web pages. The HTML document is downloaded immediately after a visit and proceeds to install itself without a user's conscious request (Van Lam Le, Gao, and Komisarczuk 2013, 49). After installation, the drive-by-download file exploits vulnerabilities in the infected system, and connects it back to the botnet.

Trojan & Worms are the underlying attack vector hidden behind drive-by-download and email and messaging infections. Trojans[3] carry malicious payloads concealed in otherwise harmless content, such as screensavers, media, and office files, whose installation is made possible by end-user flawed authorization (Shadowserver 2016). Conversely, worms have the capacity to promote self-installation and self-replication, requiring low user-interaction (Shadowserver 2016), and therefore posing a more serious risk. Worms will automatically spread through a system and attempt to contaminate other networks by distributing copies of itself via emails, social media, and P2P applications (Microsoft 2015, 140).

Email and Messaging, although not representing a technique, but rather an environment or means for carrying out an infection, are simplified but prevalent botnet vectors (Kaspersky Lab 2013). In addition, messaging services incorporated in social-media platforms as well as over-the-top (OTT) services[4] might be targeted by botnets for delivering unsolicited communications (spam) and ads. In order to benefit from these communication channels, botmasters may include malicious attachments, URLs containing malware, and other infection vectors that will compromise the device and integrate it to the botnet.

3.2. How botnets become profitable

Botmasters have found various ways to monetize the use of botnets. Here I discuss the most common revenue streams, the means by which botmasters profit from their criminal activities. These include, but are not limited to, DDoS attacks, keyloggers, click-fraud, bitcoin mining, ransomware, and toolkits.

DDoS OR DISTRIBUTED DENIAL OF SERVICE is a flooding mechanism for interrupting network services. By orchestrating a tsunami of supposed legitimate traffic, DDoS attacks hog both users' and targeted network's bandwidth (Tariq, Hong, and Lhee 2006, 1025). DDoS attacks thus compromise the target system's bandwidth, thereby weakening its capacity to respond to user requests. When successful, DDoS attacks bring down the target for a certain period, an interval in which anyone trying to access the victim's system will receive a 'denial of service' message. A common purpose behind DDoS is extortion: criminals request a ransom be paid for the DDoS to stop (Jacobson and Idziorek 2013, 124). Because of their size, botnets are capable of launching impressive DDoS attacks and extort high profile business and government institutions.

KEYLOGGERS are ingenious forms of malware designed to track information typed on a device (Kaspersky Lab 2016). For their capacity to monitor user behavior, keyloggers are deployed for capturing sensitive information shared by victims with a trusted source, such as passwords and personal data exchanged with employers, government authorities, and e-commerce services. Once in possession of these data, criminals may exploit the information to defraud victim's financial, commercial, and intellectual assets or use them to blackmail users online.

CLICK-FRAUD is a type of online scheme targeting the online advertisement industry. Web advertisement is a multilayered environment where an advertiser rewards a publisher, the owner of the page where the ad is displayed, if a visitor of the publishing website clicks on the ad during the visit. However, this multimillion-dollar pay-per-click (PPC) system has fallen victim to bot click-fraud, where the collection of bot devices is commanded to click on ads published by the botmasters or by a publisher connected to the botmasters. Advertisers are thus lured into paying for artificial volumes of bot clicks believing these are human users interested in the content advertised. Click-fraud could account for almost 10% of all ad clicks (Pearce et al. 2014, 1), potentially costing advertisers hundreds of millions of dollars annually. For instance, the notorious ZeroAccess botnet (2012) had a click-fraud facet that could monetize up to 2.7 million USD per month (SOPHOS 2012, 45–46).

BITCOIN MINING is a computer-process by which a 'miner' is rewarded for solving a blockchain cryptographic puzzle (Eyal and Sirer 2014, 436).[5] Successful miners are compensated with newly issued bitcoins and a transaction fee, a very lucrative activity considering the market value of bitcoins (1 bitcoin = 395USD on Jan 27, 2016).[6] Because in theory anyone can mine bitcoins and will be rewarded for that, the mining system is believed to promote a democratic distribution of the currency (Eyal and Sirer 2014, 436). However, given the large volumes of processing power found in botnets, mining became another business opportunity for criminals. Botmasters may now program their zombie network to mine bitcoins, creating their own mining pools and being rewarded for that.

RANSOMWARE have evolved as a category of scareware, a specific group of malware used to manipulate people's fear of private information disclosure, data erasure, and hardware damage (Kharraz et al. 2015, 1). Ransomware in particular are designed to restrict one's access to information stored in an infected device in exchange for a 'ransom'. Forms of ransomware have been known since the early 2000s, but became increasingly popular after Cryptolocker, a botnet-distributed-malware designed to encrypt victims' files and demand a fee for releasing its encryption key. In another famous case, Cryptowall allegedly

affected 850,000 computers worldwide, holding victim's files for a ransom fee typically between 200USD to 1000USD (FBI 2016, 6).

Toolkits are computer programs devised to setup malware by a third-party, often a buyer who purchased the kit in the underground market. Botnet toolkits, in turn, serve the same purpose and allow third parties to program and control their own botnets. The introduction of toolkits has arguably democratized the cybercrime industry, as they enabled non-skilled users to deploy the same category of crimeware used by expert criminals. The sale of botnet toolkits is an added layer to the monetization of botnets, as the third-party botnet is often a profit-driven effort itself. The danger posed by toolkits is the popularization of a botnet's modus operandi. Infamous botnet families have been popularized via toolkits, the most telling example being the ZeuS, whose code is openly available online.

3.3. How industry may intervene

A multitude of techniques has been created to prevent and stop botnet attacks, as well as special tools for removing the infection. Given the diversity of means and instruments for dismantling botnets, which range across prevention to immunization, I speak of four pillars of botnet mitigation in which industry can participate, viz. (1) prevention, (2) information exchange, (3) disruption, and (4) disinfection efforts.

Prevention entails the set of actions taken to hinder the integration of devices into a bot network. This includes legal, public policy, organizational, and technical measures that could foster detection, security-by-design (SBD) and awareness raising. For instance, industry may prevent botnets by installing detection tools that scan for known forms of infections. In addition to network monitoring, detection can grow outside the organization through the sharing of information (e.g. alerts and newsfeeds shared in the sector or with additional stakeholders). SBD, in turn, builds upon the concept of resilience and the goal of strengthening security from the very level of conception and design, thereby institutionalizing security within information systems (PRIPARE Project 2014, 12). The SBD model is particularly important in that it transfers the burden of rational cybersecurity choices to the experts involved in the development of the information systems. Arguably, these agents are in the position to make crucial choices about the security of the systems they produce. Supporters of the SBD model defend it can deliver an end-to-end approach to cybersecurity, as the internalization of security at the stage of design contributes to a culture of security by default (Cavoukian and Dixon 2013, 1). Certainly, SBD has its limitations. The components of a device are only as secure as the knowledge of their developers, meaning their security is always limited by the state-of-the-art. Awareness raising refers to the set of educational activities designed to promote a culture of cybersecurity against botnets. This encompasses both internal actions, such as capacity building courses and discussions inside organizations, as well as external actions aimed at raising the level of attention, interest, and skills of stakeholders, including civil society, about cybersecurity habits (a.k.a. cyber hygiene) that protects end-users and their devices from falling trap into botnets.

Information Sharing entails the exchange of data that can be relevant for taking action against botnets, what encompasses information about perpetrators, infected machines, and victims of botnet attack.[7] Information exchange environments are built

upon collaboration in the same sector, industry, or even across public and private-sector entities. The advantage offered by these channels is the opportunity to provide various actors with information captured by trusted partners, data that otherwise would not be available to them. Because botnet infections and attacks permeate various services of the Internet industry, a single actor holds limited information about the broader picture of the contamination and the potential attack. These collaborative platforms allow for the exchange of pieces of critical information and correlation of these data, providing a bigger picture of the threat and facilitating prevention and response to attacks experienced by partners. Information exchange involving industry may take the form of public–private and private–private partnerships. The first, public–private networks, are collaborative efforts created by either government or industry and count on the participation of both public and private sectors. By Tropina and Callanan (2015, 16), public–private partnerships tend to receive a greater deal of State intervention instead of cooperation, leaving industry with the most burdensome part of the deal. This asymmetry could be one of the reasons why public–private partnerships against cybercrime are less prominent than private–private partnerships. The latter have a narrower scope: they are circumscribed to a set of private actors and devised to respond to their needs. To this end, private–private partnerships are often easier to found, for their members share similar interests and duties. Nonetheless, these groups may also end up restricted to a small portion of the industry, tackle only a set of concerns particular to the group, and do not disclose valuable information to third parties. Here the issue of ensuring adequate safeguards are in place is a concern (Tropina and Callanan 2015, 33), as the lack of public sector and civil society oversight may translate into lack of accountability (see Section 4.4).

Disruption stands for the broad range of actions that purposefully disturb an ongoing botnet infection or attack. The cybersecurity community has developed a broad set of mitigation techniques that exploit various ways to detect, map, observe, analyze, and disrupt botnets. Two main categories of disruptive techniques exist, depending on the level of interaction and intrusion performed by the anti-botnet tool, namely passive and active. Apart from technical tools, legal measures can also disrupt botnets, when these actions are directed at limiting perpetrators' access to information systems, for example, via custody and imprisonment. However, while disruption of botnets combined with prosecution of cybercriminals (and later imprisonment, when applicable) can interrupt botnet activities, the backdoors will remain open (and could be misused by another criminal) until the bot devices are cleaned and vulnerabilities are patched. Therefore, an effective response to botnets must imply a comprehensive set of technical, legal, and education measures. Yet, because the private sector is better positioned and equipped to collect information about infections, victims and attacks, the activities of law enforcement as well as disinfection campaigns must be supported by the Internet industry. Multiple examples of successful consortiums involving the Internet industry and law enforcement illustrate the effectiveness of this hybrid approach. In fact, public–private efforts have delivered some of the most impactful coordinated actions against botnets in recent years (EUROPOL 2013, 2015; FBI 2014).

Disinfection is the series of mechanisms designed to remove malware contamination. It includes the cleaning or removal of a bot infestation, as well as the patching of the vulnerability exploited by the infection (immunization). Clearly, a disruption effort is

not complete before the machines are cleaned and immunized from similar infections. Despite the importance of disinfecting machines, there is no consensus on how infected users can be informed of their condition in a privacy-friendly way, nor if and how users could be compelled to disinfection by automated means. Consequently, there is a significant need for legal scholars to investigate and define the legitimate boundaries for law enforcement and private sector to issue privacy-compliant infection notices. Another obstacle to disinfection is that it can take a long time for all machines to be disconnected from a botnet. A valuable example is the case of Conficker botnet (Asghari, Ciere, and van Eeten 2015), for which a patch was made available more than 7 years ago. Notwithstanding the major disinfection efforts carried out by the Internet industry in the past years, almost a million devices remain infected to today (Asghari, Ciere, and van Eeten 2015, 1).

4. Obstacles faced by the internet industry

As noted by Asghari (2016, 42), the persistence of botnets can be traced to the fact that end-users, whose machines are compromised but act as an intermediary for the botnet attack, do not bear the full costs of the infection. Because the effects of botnets attacks are born by their final targets and society, end-users who could play an important role in mitigation do not have the incentives to protect their devices. As a result, the Internet industry actors that are suffering the impact of botnet attacks are the most willing (or compelled) to take action against the menace.

The challenges of involving the Internet industry, however, are numerous. Regulators who embrace the idea that Internet industry intervention is a key element to mitigation must attempt to overcome the challenges below. These could be summarized in lack of legal grounds for and legitimacy of intervention, legal uncertainty in relation to liability, lack of transparency and accountability, and fear of regulatory capture.[8] Extra hardships could be added to the list, but the following sections offer a sufficient overview of the main problems regulators will face when attempting to further private-sector participation against bot attacks.

4.1. Lack of legality and legitimacy

The problem of leaning on Internet industry participation to respond to botnets is the illusion that private sector's means to counter attacks are accompanied by the right to launch such countermeasures. Put differently, private sector might hold the means to counter cybercrime, but lack undisputed legal authority to do so. For instance, European Union Law does not require Internet intermediaries, let alone manufacturers and software developers, to detect malicious botnets operating in their networks. As a result of this legal void, anti-botnet actions are conducted largely on a voluntary basis and a debate on the legitimacy and eventual legality of these measures in found wanting by legal researchers. The legitimacy of these actions remains unascertained: it is not yet clear to what extent the interested parties and society are willing to give allegiance (Morgan and Yeung 2007, 11) to Internet industry intervention against botnets. Moreover, their legality within EU law is also unclear, as no thorough analysis investigating whether the launch of such countermeasures is in accordance with the law has been conducted.

Even when encouraging industry to secure their networks, the rights and duties established by legislation might be distributed unevenly across Internet industry actors and fail to address the issue of botnets directly. The legal gap is widened when examining the laws applicable to disinfection procedures and exchange of information among interested parties. As it turns out, many of the agents that could counter botnets lack a legal basis to do so, and those who might have legitimacy to counterattack may find the legal requirements too narrow, unattainable, or imprecise. For instance, in light of current EU legislation, Internet industry countermeasures against botnets are neither clearly lawful nor forbidden, as some actions are regulated partly and others remain in legal oblivion. Furthering Internet industry participation without a proper advancement in regulation would be far from ideal: any attempt to improve Internet industry intervention must be followed by regulation that is not only effective and legitimate, but also optimal in terms of design.

4.2. Unclear liability rules

Liability refers to the criminal and civil responsibility that arises from a behavior in conflict with the law. As noted by Dunn and Mauer (2006, 20), in a monopolized state, allocating responsibility in the hands of state actors is the norm, whereas in a liberalized economy it is not clear who should bear the costs for installation, security, and maintenance of information networks. The lack of legality, coupled with the absence of clear liability rules in information security have created legal uncertainty for companies working on networks affected by botnets. The main peril faced by these actors is to have their countermeasures classified as an offense, be it a civil wrongdoing, a criminal offense, or a human rights violation (if one adopts the theory of horizontal effects of fundamental rights).[9]

The choice to deploy a disinfection tool is a telling example of how the absence of tort laws and clear liability rules makes intervention against botnets a risky decision for the industry. In general, disinfection can be promoted in a voluntary or compelled basis. In the first case, Internet industry actors might notify users they have been infected and inform victims on means to remove the contamination. In the second case, the Internet industry might restrict user access to their services until the machine is no longer compromised. In both cases, automate cleaning tools insert code to repair the backdoor exploited by the botnet. By current legislation passed at CoE level, however, attempting to clean a botnet infection through patching code may constitute a cybercrime offense, because such disinfection mechanism is technically similar to tools used for hacking, data interference, and system interference. In an effort to remain technologically neutral, the CoE Cybercrime Convention did not distinguish between attacks and mitigation techniques. As a result, deploying mitigation tools may be considered a criminal offense and the agents criminally liable for the wrongdoing. In addition, if the disinfection tool hurt users' access to services, software, or even their own machine, the actor responsible for the disinfection may be liable for such unexpected damages.

Moreover, the actions connected to mitigation tools may translate into human rights violations. Anti-botnet actions are often connected to the processing of data and interruption of services of those flagged as potential threats. While the occasional processing of personal data for the purpose of mitigation might be justified, the strategies delineated in section 3.3 often comprise large-scale collection, analysis, and distribution of data by

various actors interested in countering botnets. The legal boundaries of the data processing occurring in this multilayered environment, however, have not been duly assessed. The ACDC project (2014), which attempted to launch a pan-European clearing house expediting information sharing on botnet mitigation, flagged the existence of several legal hurdles connected to privacy and data protection and the narrow grounds by which the processing envisioned by the technical solutions could be compliant with the EU legal framework.

In the language of human rights, botnet mitigation may hinder the exercise of the right to privacy, data protection, and to receive and impart information. Moreover, a detailed examination of how effective mitigation can be reconciled with the law is lacking. Internet industry intervention against botnets threatens human rights in three significant ways. First, there is a danger that mitigation tools and strategies are created and launched with a result-oriented approach, overlooking the need to make countermeasures compatible with privacy, data protection, and the right to receive and impart information. Second, in the absence of legal grounds, the actions of the Internet industry might directly violate these same fundamental rights. Thirdly, without proper transparency and accountability, companies would have no incentives to lessen the impact of their tools or to adequate their behavior to the law.

The absence of clear liability rules may thwart accountability of public–private partnerships in a more severe manner. If Carr (2016, 43) is correct in affirming that private sector tends to refuse liability when undesired results emerge from cybersecurity efforts, such as compensatory damages incentivizing the engagement of the Internet industry may have the drawback of fostering a model in which the supported agents avoid liability for their actions. In this case, regulation may be the necessary mechanism to reestablish protection and realization of rights.

4.3. Lack of transparency

From a societal perspective, Internet industry participation in battling botnets could also hurt expectations of transparency. Transparency is defined as 'the principle of enabling the public to gain information about the operations and structures of a given entity' (Etzioni 2010, 389). Traditionally, the fight against crime has been a task of the State, where society has acted as an observer of the conduct, behavior and results of the actions led by the government ('transparency downwards') and held public agents accountable for them (Heald 2010, 29). This same expectation of transparency could be frustrated in case private sector starts fighting botnet crimes, for transparency is mostly understood as a concept applicable in relation to public authorities or private-sector activities vested in a public function (Scott 2000; Hood and Heald 2010; Etzioni 2010; Baldwin, Cave, and Lodge 2012; Lodge and Wegrich 2012). If Internet industry actors were lawfully allowed to launch countermeasures against botnets, would they be required to make their actions transparent to society?

The answer is yes. The principle of transparency, which encompasses the idea of accountability towards a certain group, need not be limited to the activities of public authorities in public law (Buijze 2013, 30). Let us first contextualize Mock's definition of transparency ('a measure of the degree to which the existence, content, or meaning of a law, regulation, action, process, or condition is ascertainable or understandable by a party with

reason to be interested in that law, regulation, action process, or condition') (2013, 30) in the environment of botnet mitigation. According to Mock (2013, 30), transparency is a measure that comes into play when the actions of a certain party prompt the reasonable interest of a third party on those specific actions. Considering that botnet countermeasures pose a risk to citizens' rights, as argued throughout this study, users whose rights are impacted or likely to be impacted by such measures hold a reasonable interest in gaining further information about such measures. As a result, private-sector entities launching anti-botnet actions should make their actions transparent to their stakeholders. In fact, the concept of transparency has become omnipresent in business activities around the globe (Weisband and Ibrahim 2007, 9) – even if mostly under the umbrella of Corporate Social Responsibility. The challenge presented to the regulator thus is to determine standards of transparency applicable to the activities of Internet industry actors, as well as to create mechanisms that guarantee respect for transparency. Without transparency standards, Internet industry participation might be detrimental to democratic governance: society will be partly reliant on private sector for the offering of cybersecurity but have insufficient access to information that is directly relevant to individuals.

4.4. Lack of accountability

Similarly to the lack of transparency, absence of accountability in relation to anti-botnet efforts could hinder democratic governance. Much like transparency, studies on accountability are no longer constricted to the realm of public governance, even though its concept remains notoriously imprecise (Mulgan 2000, 87). Following a decentered approach to regulation and the expansion of private-sector powers, accountability will be taken to refer to 'the set of mechanisms and processes that impose an obligation to reveal, to explain and to justify regulatory actions (… .) [accountability] involves the identification of who is accountable, to whom, and for what' (Morgan and Yeung 2007, 11) and implicate both state and non-state agents.

By Mulgan (2000, 87), accountability arises from a duty one performs in relation to another and in face of the threat posed by her actions on the rights of this other. If we assume that Internet industry actors have at least a duty to care for their networks and customers, then there is no reason why they should not be held accountable for the threat these countermeasures might present to the rights of Internet users. Other scholars corroborate this perspective by affirming that private companies are accountable for their actions not only to stockholders but also to customers and the community (Weisband and Ibrahim 2007, 10–11). So far, it has been determined that Internet industry actors (who) are accountable to Internet users (whom), but the nature of this accountability, more precisely what it involves (accountable for what?) is less precise.

Investigating the differences between accountability in the public and private sectors, Mulgan (2000, 87) defends that, since accountability arises from a responsibility, it entails the obligations of accounting for the performance of this duty and accepting sanctions and redirections in relation to its performance. To this end, the enforcement of these two obligations ((1) to perform a duty and (2) to accept sanctions and redirections) might be sought through the particular and general stances (Mulgan 2000, 88). Particular accountability refers to individual redress in case a specific decision taken by the organization affects that precise citizen (Mulgan 2000, 89). General accountability, in turn, comes

into play when the broader community questions the general policy and decision-making adopted in the organization (Mulgan 2000, 91). Both stances are applicable to the Internet industry, for botnet countermeasures seriously affect the rights of specific users (e.g. those flagged as victim or authors of a botnet infection, in addition to those whose connections are monitored in search for malicious behavior) and society. The lack of accountability places the trustworthiness of the functioning of the Internet at peril, and could be questioned by individuals, business, and governments alike.

In spite of the serious impact Internet industry actors may have on the Internet community, the controls exercised over the performance of private-sector activities are less stringent than the controls applicable to public authorities (Mulgan 2000, 88–89). Once again, it is the task of the regulator to sanction and enforce standards of accountability applicable to the actions of the Internet industry. The absence of accountability rules enhances the risks posed by Internet industry intervention: without clear accountability controls, the participation of the Internet industry may create a legal and public policy void in which the rights and freedom of citizens are threatened, but no one would be held accountable for such harm or be subjected to public scrutiny and sanctioning.

4.5. Regulatory capture

Understood broadly, regulatory capture refers to the process through which special interests affect regulatory intervention (Dal Bó 2006, 203). Carpenter and Moss (2013, 13) define capture as the result or process by which regulation is consistently or continually directed away from the public interest and toward the interest of the regulated industry, by the intent and action of the industry itself. Previous works in the field of regulatory capture have found that the phenomenon is more likely to happen in concentrated industries, given that politicians are inclined to favor these key corporations in exchange for political support (Lodge 2014, 539).

It is unclear how concentrated the Internet industry is, but in comparison to oligopolies, the environment where regulatory capture is mostly observed (Dal Bó 2006, 204), the Internet industry sector in the select countries whose initiatives are analyzed (NL, DE FI, and US) seems non-monopolized. Yet, even if the likelihood of regulatory capture is potentially reduced in horizontal markets, the risk persists. The network regulation model that is so typical to the Internet emphasizes the influence network regulators have in a broader group and as such runs the risk of being captured by the private interest of such nodal regulators (Baldwin, Cave, and Lodge 2012, 65). This is applicable to the relations between Internet industry actors. Moreover, the network regulatory model pays scant attention to the imbalance of powers between actors involved in the network of regulators. As a result, if no measures are internalized for curtailing polarization in the network of regulators, large corporations may overshadow the contribution of smaller players.

Among the proposed solutions to minimize the regulatory capture, Dal Bó (2006, 220) mentions (1) the creation of bureaucratic procedures that allow various stakeholders to share information about the regulatory process, the (2) creation of legislative committees that specialize in monitoring regulators, and possibly (3) the creation of consumer advocate groups. In this study, the suggestions of Dal Bó could be construed for (1) establishing transparency mechanisms for stakeholders' policy-making decisions, (2) launching a

multistakeholder committee to monitor the actions of regulators (state and non-state agents), and (3) creating a public interest group to exert pressure against capture (Lodge 2014, 541).

5. Regulating internet industry's participation

What is regulation and who regulates social behavior? Scholarship pontificates various answers to this question, answers that are heavily contingent on the perspective adopted by the scholar. This paper embraces regulatory pluralism, or the school of regulation theory which conceives regulation as 'all forms of standards, formulated by the state or not, with the purpose of controlling social behavior' (Morgan and Yeung 2007, 3). The rise of non-state actors from the periphery towards the center of the regulatory debate has reshaped the field of regulation, which now largely recognizes both public and private actors as sources of regulation (Lodge and Wegrich 2012, 16). This new perspective of regulation is based on horizontality between regulated and regulators, and resonates with our cybersecurity ecosystem. The combined effort of various actors that, each at their own capacity, influence the functioning (and security) of the Internet and obey to a wide variety of regulatory instruments, is the moving force behind cybersecurity. The idea that individual governments cannot ensure cybersecurity without the support of private sector, has become 'conventional wisdom' (Tropina and Callanan 2015, 14).

In light of the above, any attempt to regulate the actions of the Internet industry must consider the contribution of these same actors as regulators. Conversely, attempts to pass regulatory instruments that do not involve the Internet industry (as regulators and/or regulated), are likely to be ineffective, given that such actors control much of the infrastructure through which botnets propagate. In the following sub-sections, I discuss the initiatives enacted in the Netherlands,[10] Germany,[11] Finland,[12] and the US,[13] pioneering countries in promoting Internet industry participation in the fight against botnets. Later, I examine the value of using a regulatory compass based on responsibility as a tool for supporting regulatory activity. Finally, I explore a set of regulatory means (codes of conduct, guidelines, and legislation) that could support Internet industry's involvement in botnet mitigation.

5.1. Pioneering efforts across the globe: NL, DE, FI, and the US

Anti-Botnet Initiatives (ABIs) have proliferated in the past decade following a polycentric strategy to reduce the impact caused by botnets. In general, ABIs rely on the Internet industry as the chief actors in successful botnet mitigation. The following paragraphs briefly describe the ABIs enacted in the NL, DE, FI, and in the US The selection of countries and initiatives, as previously stressed, is founded on their pioneering character and the influence they have exerted in other countries.

ABUSEHUB [NL] acts a clearinghouse for collecting and analyzing abuse data on infected machines in the Netherlands. The main objective of this private–private partnership is to reduce the bot infection levels in the country, thereby increasing trust in the Dutch digital industry. At the time of writing, Abusehub consisted of nine national ISPs, the .nl registry (SIDN), and the national research and education network operator (SURFnet). In a research funded by the Dutch government to evaluate the performance

of the private-sector ABI, researchers from TU Delft found the ISPs part to AbuseHub presented a steeper rate of clean machines in comparison to ISPs who were not part of the ABI (Moura et al. 2015). The active participation of these ISPs in a forum for exchanging botnet intelligence is reported as a possible cause for the decrease in infection rates (Moura et al. 2015), what has fostered the hope that further anti-botnet efforts led by the Internet industry would translate in similar positive results.

BOTFREI [DE] was launched in 2010 as an effort led by ECO, a large association of German ISPs and other Internet industry actors, and is funded by the German Ministry of Internal Affairs (Botfrei sd). After the widespread contamination of Conficker botnet and the worrying levels of infections in the country around 2010, national authorities and industry created the concept behind Botfrei, which operates as a centralized platform for collecting and disseminating data about botnet infections affecting its members (Botfrei sd). Botfrei reports that the actions led by its partners have massively contributed to reducing bot contaminations in Germany, and one of the reasons why the nation is no longer ranking among the top infected countries in the world (Botfrei sd). The functioning of Botfrei has three stages: input, analysis, and output data. All members are invited to send input data about bot infections affecting their networks, but dissemination of output data is controlled. Once shared with Botfrei, input data are further analyzed at a centralized clearinghouse and then redistributed to stakeholders in accordance with their IP range and legitimate interests over the data. In addition to this industry-oriented approach, Botfrei hosts a free platform for users to scan their devices for infections.

AUTOREPORTER [FI] is a Finnish initiative launched in 2005 and offered in the form of a service by the national Computer Emergency Response Team (CERT) (CERT-FI), now part of the National Cyber Security Centre Finland (NCSC-FI). The service performs an important task in alerting the network of major Finnish ISPs on any information about security incidents affecting their network, as detected by the national CERT (CERT.FI) (Grenman 2009). This automated service has become a valuable tool to the Finnish cybersecurity community (Grenman 2009) and inspired similar efforts in EU member states. One of the reasons why AUTOREPORTER is able to operate under the Finnish framework is the broad scope of attributions held by CERT-FI. The competencies of the national CERT comprise resolving cybersecurity incidents, as well as collecting and disseminating data about cybersecurity threats (Viestintävirasto 2016) that may be relevant to the Finnish community.

M3AAWG or the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) [US] is a private–private partnership among US Internet industry actors (but also foreign companies) working against various cybersecurity threats and, in particular, botnets. M3AAWG comprises more than 200 members worldwide and strives for self-regulatory measures in the field of cybersecurity by establishing best practices and guidelines. Among the relevant documents led by M3AAWG is the voluntary anti-botnet code of conduct for ISPs enacted in the US, formally known as the US Anti-Bot Code of Conduct (ABCs) for ISPs.[14] The instrument is the result of a public–private multistakeholder discussion (Communications Security, Reliability, and Interoperability Council) which involved several M3AAWG members and the US Department of Homeland Security. As a voluntary code, it attempts to set up best practices and encourage private-sector commitment to botnet mitigation.

5.2. Spectrum of responsibility

The initiatives described previously offer a practical insight into the activities of regulators in NL, DE, FI, and US, states pioneering coordinated multistakeholder-efforts against botnets. Yet, regulators are compelled to make analytical decisions based on clear standards. To that end, this section presents a 'Spectrum of Responsibility', what may serve as a regulatory compass for guiding regulatory choices based on reasonable expectations of responsibility distributed across the Internet industry. If we are to understand that Internet industry actors have the potential to contribute to anti-botnet actions, it is paramount to ascertain the responsibilities that each set of actors should bear and, equally importantly, in which order. Establishing such a divide will facilitate regulatory choices in regulating anti-botnet actions by industry, as it provides a yardstick to differentiate between actors in the sector.

I shall argue that although the substance of the responsibilities of each Internet industry actor is defined by national legal systems, the hierarchical order that influences the allocation of responsibilities across the Internet industry is of technical nature and can be predetermined. Information networks operate in the architecture defined by engineers and attempting to impose norms that contradict such framework may be in vain and result in regulatory failure. An effective spectrum of responsibility for the Internet industry must respect the architecture of information systems network and consider the means and opportunities that each set of actors possesses within this technical structure.

Establishing a spectrum of responsibility is to recognize the existence of duties across different private actors. In other words, a spectrum of responsibility is a form of regulation. In the context of this paper, I am interested in a spectrum of responsibility that could be used to understand the different expectations society could have in relation to private-sector behavior. The actors first called upon to perform their assigned duties will be expected to act accordingly before the same is requested from an actor positioned later in the chain. Clearly, this line of thought is only reasonable insofar as such as duty to act (or not to act) exists. In the case where such a duty exists, the chain of responsibility turns into a de facto spectrum of subsidiary and/or joint forms of liability. For the time being, I shall assume such a duty could exist for all actors included under the expression 'Internet Industry'. This affirmation arises from the assumption that all Internet industry actors described in this paper can contribute, in a variable scale, to botnet mitigation.

The technical architecture of the Internet could be described through the Open Systems Interconnection (OSI) model. The OSI model conceptualizes the functioning of information systems into seven layers, ranging across Application, Presentation, Session, Transport, Network, Data Link, and Physical layers (SANS Institute 2001, 2). Each layer performs a dedicated function within the system and condenses the data flow transmitted to the following level. The OSI model has inspired different regulatory systems across disciplines, including law. These systems are traditionally based on the concept of vertical regulation and the butterfly effect promoted by changes at 'higher layers'. Benkler advocates that regulation affecting the basal layers of vertical regulation would naturally echo throughout the higher layers (Murray 2007, 75). This stratified model recognizes physical infrastructure, logical infrastructure (the so-called 'code' layer, according to Lessig (2006)), and content layers, in this decreasing hierarchic order (Murray 2016, 37). Even if simplistic, the model implies that when attempting to regulate content online, a measure applying at

the infrastructure or code level would be an effective means to achieve the final result, for the repercussion of the measure would implicate the lower layer (content) all the same.

Building upon the reverberation effect identified in Benkler's earlier studies, where a change in a higher layer resounds through the lower layers, Domanski (2015, 10) suggested a new addition to three-layer stratification system, which would result in a four-layer system comprised of infrastructure, technical protocols, software applications, and content. The subdivision of the code layer into technical protocols and software applications, defends Domanski (2015, 10), is relevant in that the actors behind these two code layers are very distinct from each other and deserve to be addressed separately. I sympathize with Domanski's view, but am not convinced code developers must be split into two single layers. In light of the above, I contend any form of regulation intended to ascertain cybersecurity responsibilities of the Internet industry should respect the hierarchical chain of Internet Governance, code development, and online content, pondering the means and opportunities available to each set of actors. Therefore, this paper presents a spectrum of responsibility for botnet mitigators influenced by their hierarchical position in the three-level pyramid proposed by Benkler. That being said and in light of the set of actors defined here, our spectrum of responsibility should resemble the following stratification (from high to low):

(1) Physical Infrastructure: hardware manufacturers.
(2) Logical Infrastructure/Code: Hosting Providers, Domain Name Registrars, Software developers, application developers, ISPs.
(3) Content: Online content providers, Online Search Engines.

There is no obstacle to creating subdivisions into the three layers above, thereby defining a sub-order to be followed within each layer. However, it seems reasonable to leave any such subdivision to a concrete analysis of the case at hand. This is because the diversity of botnet operations may translate into shifting responsibilities among actors in a given layer. The modus operandi of a botnet affects the expectations about which actor must react and at what moment, and thereby influences the distribution of responsibilities in the same layer of stratification. For now, the argument is concentrated in ascertaining that a spectrum of responsibility presupposes the existence of a duty of care and, following the architecture of the Internet, the allocation of responsibility is partly shaped by the hierarchical chain of the Internet itself. Thus, regulation pertaining the distribution of liability and responsibility among Internet industry actors must align public policy goals to the limitations posed by the protocols that govern the functioning of the Internet.

5.3. Soft law: self- and co-regulation

This section argues that regulators should consider the use of soft law as a means for regulating Internet industry activities in botnet mitigation. Legal scholars often divide the landscape of regulation into the binary system of hard and soft law regimes. While it is possible to identify a wave of regulatory mechanisms flowing in between categories, regulation is mostly either legally binding (hard law) or deliberately non-binding in character but legally relevant to the adopting parties (soft law) (Skjærseth, Stokke, and Wettestad

2006, 104). Because soft law is often a tool for presenting forms of self-regulation, cybersecurity actors who oppose strict regulation and want industry-centered norms have preferred soft law mechanisms and self-regulation of their activities.

I argue that the flexibility of soft law is possibly better suited to regulating certain elements of Internet industry participation against botnets than its hard law counterpart, for soft law instruments offer greater room for progressive adaptation and a more inclusive approach to regulation, allowing for various forms of consensus-based norms. In addition, soft law tends to adopt a more tolerant perspective on sanctions, often regarded as factors that can undermine adherence to norms. One characteristic of soft law instruments, which can be beneficial to the voluntary character of Internet industry collaboration in fighting botnets, is the possibility of adopting constructivism towards compliance. In this model, failure to abide to the norms is followed by a supportive approach in which the infringing party receives the help needed to achieve compliance. In contexts in which no legal obligation to adopt a certain conduct exists, such as many of the actions that the Internet industry could undertake to mitigate botnets, constructive models may encourage participation and promote regulatory effectiveness.

Morgan and Yeung (2007, 92) argue in favor of self-regulation as one of the distinctive modalities for regulating citizen-behavior. By the British authors, self-regulation (or consensus) differs from other forms of regulation 'on the basis that the mechanism through which behavior is influenced and constrained rests primarily on the consent of its participants' (Morgan and Yeung 2007, 92). Because in consensus-based rulemaking regulatees are able to actively shape a field in which they have specialized knowledge and act daily, the outcome is expected to be more effective too (Morgan and Yeung 2007, 93). Self-regulation is thus a potential tool for regulating participation of the Internet industry in botnet mitigation owing to the fact that if industry is allowed to proactively determine the means and mechanisms, as well as the consequences of collaboration, regulation could translate the views of regulatees and thereby potentially boost levels of compliance and regulatory efficacy.

The term co-regulation refers to regulation built upon the joint effort of state and non-state actors. Lodge and Wegrich (2012, 105) define co-regulation as a non-state regulatory framework constructed to achieve public policy goals and grounded on clear state-based laws. Co-regulation is thus understood as state-sponsored self-regulation, where institutional authorities delegate decision-making to industry in the hope that such effort may translate in enhanced compliance, expertise, and effectiveness. In fact, the difference between industry self-regulation and co-regulation is a matter of how these forms of regulation are initiated. In the first, industry organization is the leading force behind decision-making. In the latter, the state has a clear intention to enact regulation in a given field where industry has pivotal influence and therefore encourages industry to take over the decision-making process. For the purpose of the public policy goal pursued in this paper, namely increased cybersecurity, differentiating between these two forms of self-regulation is marginally relevant, and the reason why the broader term 'self-regulation' will be preferred, but shall be interpreted as a wider concept that encompasses both industry self-regulation and co-regulation.

Despite the possible advantages of self-regulation, its use in cybersecurity could generate inadequate incentives to regulatees, derail into regulatory capture, and promote an industry race to the bottom. As discussed by Lodge and Wegrich (2012, 105), self-

regulation is a self-enforced system in which the absence of a trustworthy enforcement system reflects on lack of accountability and effectiveness. In order to work, self-regulation requires a strong industry commitment to compliance, but when industry itself is responsible for monitoring violations and imposing sanctions, conflicts of interest may interfere with the rightful application of the norms in detriment to public policy goals. Even so, the threat of inconsistent enforcement should not be sufficient to exclude the capacity of self-regulation to achieve greater effectiveness than hard law frameworks in select scenarios. In a top-down approach, command instruments are often victim of excessive terminological vagueness, punishment-oriented justice, and lack of regulatees' participation. In the case of botnets, where the infection and attack channels are under the control of private sector, the voice of the Internet industry cannot be disregarded and should be given, arguably, detailed consideration. Yet, this voice can only shape regulation if a reliable enforcement system is set up and if industry actors actively participate in the process of self-regulation. Self-regulation is more likely to succeed where industry is united by a collective interest, regulatees have formed a trust circle, clear objectives have been set, consumer and citizen expectations are met, and normative enforcement is feasible (Tropina and Callanan 2015, 35). If those conditions are present, self-regulation may prove to be the most effective form of regulation. In a scenario where those circumstances are met, I argue that both codes of conduct and sectorial guidelines are valuable elements for regulating Internet industry's activities.

5.3.1. Codes of conduct

Codes of conduct are a form of self-regulation in which regulatees define a set of norms to regulate a topic of their interest, which is not yet covered by law. Codes of conduct are voluntary in that parties are not obliged to participate in the codes or abide to them. However, if parties adhere to them, compliance should follow. By adopting such codes, business generates normative expectations for customers, governments, and civil society. This form of regulation aggregates the benefits of self-regulation and offers many advantages to signatories. This is because consensus-based norms: (1) can be used for improving corporate social responsibility reports, (2) create some level of normative certainty and expectation management in the industry, (3) act as arguments for partly shielding liability claims, as they may serve as evidence that a given actor has adopted the best practices in the industry.

In relation to botnets, codes of conduct can be particularly helpful to regulate mitigation practices at large, such as the anti-botnet code of conduct adopted by M3AAWG (US) in 2012.[15] More specifically, codes of conduct can support industry in dealing with targeted aspects of mitigation, such as botnet takedowns. The latter is the case of the Notice-and-Takedown code enacted by the Dutch cybersecurity industry in 2008.[16] A quick look at these documents, however, reveals the fragility of their terms and the superficiality of the debate over important aspects such as liability, transparency, legitimacy, reporting duties, and protection of fundamental rights. Moreover, codes of conduct could be issued to cover each of the four mitigation pillars mentioned above, therefore promoting a more consistent industry approach towards intervention. By enacting dedicated codes of conduct, the Internet industry could advance the normative expectations about their role in botnet mitigation in a more dependable manner.

5.3.2. Sector guidelines

Sector guidelines can be understood as non-binding instructional commands. They are less authoritative than codes of conduct in that they do not set commitments, but can be of great help to private actors that seek further information on how to act in a given situation. Moreover, sector guidelines are valuable in that they may address the more specific concerns of a sub-section of a larger industry group. Together, the instructive and specificity character of sector guidelines are the reasons they may become valuable tools in botnet mitigation. By designing sector guidelines, individual industry groups can discuss among peers the main issues affecting their activities. For instance, where ISPs are concerned about the tools that can be enabled to deviate a DDoS attack, registrars may worry about which techniques can detect malicious servers hosted in their domains, whereas software developers may wonder about the best practices in patching vulnerabilities. These sector-specific concerns may find no place in higher-level regulatory instruments involving multistakeholderism, but sector guidelines could be the proper venue for this debate.

As the world of botnets increases in complexity, more industry actors are likely to face sector-specific concerns. In the same way as codes of conducts, observance to sector guidelines may protect industry from liability claims, setting the baseline for the entire group of interested actors. The challenge of aligning the interests of industry to those of society, however, remains. Preventing self-regulation from deteriorating due to regulatory capture as well as promoting adherence to guidelines and their soft enforcement systems are a permanent regulatory concern. More importantly, if a government has no concrete agenda for promoting and supporting self-regulation, industry should not be optimistic about the success of their regulatory efforts either (Tropina and Callanan 2015, 18).

5.4. Hard law: the legal minimum

At the extreme opposite of self-regulation lies command forms of social control, or the enactment of rules of conduct and prohibited behavior sanctioned by law enforcement authorities (Morgan and Yeung 2007, 80). Despite my argument for self-regulation in the form of codes of conduct and guidelines, one must recognize that the success of self-regulation is contingent on many factors, such as trust, voluntary compliance, and effective and democratic participation of regulatees. In addition, there is the bare legal minimum that cannot be left to the discretion of industry, for its absence would contradict the fair expectations of society and the public interest itself. Therefore, I contend hard law intervention should cover the legal minimum, thereby regulating aspects that cannot be transacted by industry.

Bearing in mind the extent of the liability risks connected to botnet mitigation, it comes as no surprise that anti-botnet efforts have been given limited publicity. Many industry actors perceive public awareness as an increased liability risk. This is not to say that government collaboration in public–private partnerships ensures greater transparency standards. In fact, most of the EUROPOL and FBI actions undertaken in partnership with the Internet industry fail to disclose various details of the operations and to answer many of the legal questions posed by researchers in the field.

While it is not necessary to assume individuals' rights are always at risk in these operations, the absence of transparency thwarts accountability of private and public actors. Clarifications on the terms in which public and private sector are cooperating with each other and even within the same sector could contribute to bringing these arrangements to the surface, where they can be scrutinized by society. Today, the duration of cooperation, the powers of decision-making, and the rules by which risks are negotiated take place without the involvement of citizens. Moreover, the lack of legal certainty about legitimacy and liability has hampered greater involvement of Internet industry actors, thus negatively affecting botnet mitigation. To this end and considering other questions discussed in this paper, I propose the following – ideas that I intend to explore further in future research:

(1) The law must define what set of actors is crucial to the security of the Internet and recognize the heightened responsibilities this position entails.
(2) The law must should recognize Internet industry's duty to care for their network, customers, and reputation, clarifying the circumstances in which actors may exercise the right to self-defense as a means to counter botnet attacks;
(3) Public–private, public–public, and private–private partnerships or other forms of collaboration instituted for the purpose of combating botnet crimes must involve the participation of civil society organizations in their advisory board and regularly disclose reports on the actions taken by both public and private actors and how these impact the exercise of fundamental rights, more specifically the rights to privacy, data protection, freedom of speech, and the right to present a complete defense, and how the impact of these actions was duly assessed before countermeasures were launched;
(4) Civil and criminal liability for measures taken by the Internet industry with the purpose of fighting against botnets must be regulated by dedicated legislation, which shall define the standards by which countermeasures are authorized in light of the legitimate interests of the ample variety of Internet industry actors, the foreseeable circumstances of the case, and the actual negative impact caused to third parties, as well as measures to prevent spillovers on Internet users.

6. Conclusions

Enforcing the rule of law against botnets has been a notoriously daunting task, evidenced by the wide contrast between statistics on bot infections and inflicted losses, on the one hand, and the low numbers of takedowns, on the other hand. Recent law enforcement operations have attempted to overcome these setbacks by calling for support from the private sector. Owing to their expertise and strategic infrastructure, industry is well equipped to tackle botnets in a way law enforcement cannot match. The Internet industry, in turn, may benefit from these operations by having a key opportunity to defend their networks, protect their customers, and strengthen their business model. As such, both governments and companies are keen to admit that businesses, not public authorities, are in a privileged position to timely detect, prevent, and react to botnets.

Nevertheless, industry participation faces important challenges. The promises that by involving the Internet industry nations will enhance their response to botnets stumble upon criticism over the viability and legitimacy of this hybrid model of law enforcement. Concerns about expanding industry participation include the lack of transparency and accountability of Internet industry activities, unclear liability rules, fear of fundamental rights violations and regulatory capture, and the absence of sufficient incentives to ensure the companies will act in the public interest. In addition, even if considered as the crown jewel of botnet mitigation, the Internet industry may not possess the best information to decide on the lawfulness of countermeasures and thus see their activities hampered by high liability risks. Thus, without regulatory instruments that clarify these challenges, private actors may not only lack the means to adjudicate whether and under what circumstances they should respond to an attack, but also the incentives to combat botnet crimes.

In this paper, I attempted to present preliminary solutions to the bottlenecks that should be tackled by any regulator looking at furthering Internet industry involvement in botnet mitigation. By outlining forms of regulation applicable in different contexts, this study adds to the body of knowledge. It is the first of its kind to analyze the pioneering efforts of select countries, propose a framework for allocating responsibilities across the internet industry, and list a series of regulatory recommendations for facilitating responsible industry intervention in the combat against botnets. Legal literature on botnets remains scarce but the lack of a wider legal debate has not stopped the creation of several ABIs. These public–private and private–private efforts are led by the belief that such forms of intervention are beneficial to society and business altogether. Presently, actors involved in these tasks lack legal and broader regulatory certainty about their actions and are hungry for a wider discussion on their duties, responsibilities, and competences. Society, in turn, is anxious for a deeper examination of this hybrid model of cybercrime fighting. Finally, it is up to regulators to guarantee that, in the midst of this novel form of combat to criminality, public interest, legal rights, and public policy goals are properly respected.

Notes

1. However, the reliability of such numbers has been criticized. Scholars (Anderson et al. 2012) and industry researchers (Florêncio and Herley 2013) have taken exception to the methodology for measuring cybercrime costs, contending that current statistical methods are prone to biases, resulting in inflated numbers that favor particular sectors of the cybersecurity community.
2. Known as the most interconnected country of Europe, Estonia saw the activities of its presidency and parliament, government ministries, political parties, large news organizations, its biggest banks, and firms specializing in communications be severely affected by the attacks ('Russia accused of unleashing cyberwar to disable Estonia' 2007).
3. This type of malware gained its particular name for the fact that it presents itself in a misleading form, waiting for a positive reaction from the victim to reveal its harmful nature.
4. Examples of OTT messaging services include Skype, Viber, and WhatsApp, among others.
5. This monetization technique was observed in the ZeroAccess botnet (2012) (SOPHOS 2012, 11)
6. Bitcoin real-time prices are available at http://www.coindesk.com/price/
7. This could include email addresses, data about operational systems, location data, IP addresses, history of activities, pseudonyms, etc.

8. The select obstacles connected to the involvement of the Internet industry sector are the result of consultations carried during the Botleg project and literature review.
9. This study is aligned with the theory of horizontal or direct effects of human rights on third parties (Cherednychenko 2007, 5), which considers that both states and non-states actors may violate human rights.
10. Abuse Information Exchange (Abusehub): https://www.abuseinformationexchange.nl
11. Botfrei.de: https://www.botfrei.de
12. Autoreporter: https://www.cert.fi/katsaukset/tilastot/autoreporter.html
13. Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG): https://www.m3aawg.org/abcs-for-ISP-code
14. Final Report U.S. Anti-Bot Code of Conduct (ABCs) for ISPs, available at https://www.m3aawg.org/system/files/20120322_WG7_Final_Report_for_CSRIC_III_5_0.pdf
15. See https://www.m3aawg.org/system/files/20120322_WG7_Final_Report_for_CSRIC_III_5_0.pdf
16. See http://www.ecp.nl/sites/default/files/NTD_Gedragscode_Engels.pdf

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This study is fruit of my PhD research, funded by the NWO BotLeg project, a research consortium that brings together public and private sector fighting against botnets.

References

ACDC (Advanced Cyber Defence Center) Project. 2014. "D1.8 – Legal Requirements, 2nd Iteration." Accessed August 1 2016. https://www.acdc-project.eu/wp-content/uploads/2015/11/ACDC_D1.8.2_Legal-Requirements-Second-Iteration.pdf.

Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Michel van Eten, Michael Levi, Tyler Moore, and Stefan Savage. 2012. *Measuring the Cost of Cybercrime*. Berlin: Workshop on the Economics of Information Security – WEIS2012. 1–31.

Asghari, Hadi. 2016. *Cybersecurity via Intermediaries*. Delft: TU Delft.

Asghari, Hadi, Michael Ciere, and Michel van Eeten. 2015. *Post-Mortem of a Zombie: Conficker Cleanup after Six Years*. Proceedings of the 24th USENIX Security Symposium, Washington, DC, August 12–14.

Baldwin, Robert, Martin Cave, and Martin Lodge. 2012. *Understanding Regulation*. Oxford: Oxford University Press.

Brenner, Susan. 2007. "Private-Public Sector Cooperation in Combating Cybercrime: In Search of a Model." *Journal of International Commercial Law and Technology* 2 (2): 58–67.

Buijze, Anoeska. 2013. *The Principle of Transparency in EU Law*. Utrecht: University of Utrecht.

Carpenter, Daniel, and David A. Moss. 2013. *Preventing Regulatory Capture*. Cambridge: Cambridge University Press.

Carr, Madeline. 2016. "Public–Private Partnerships in National Cyber-Security Strategies." *International Affairs (Chatam House)* 92 (1): 43–62.

Cavoukian, Ann, and Mark Dixon. 2013. *Privacy and Security by Design: An Enterprise Architecture Approach*. Ontario: Information and Privacy Commissioner. https://www.ipc.on.ca/images/Resources/pbd-privacy-and-security-by-design-oracle.pdf.

Cherednychenko, Olha O. 2007. "Fundamental Rights and Private Law: A Relationship of Subordination or Complementarity?" *Utrecht Law Review* 3 (2): 1–25.

Clark, Kassidy, Martijn Warnier, and Frances M. T. Brazer. 2011. "The Future of Cloud-based Botnets?" In *CLOSER 2011 – International Conference on Cloud Computing and Services Science*, edited by Leymann, Frank, Ivanov Ivan I, van Sinderen Marten, and Shishkov Boris, 597–603. Noordwijkerhout: SciTePress – Science and Technology Publications.

Dal Bó, Ernesto. 2006. "Regulatory Capture: A Review." *Oxford Review of Economic Policy* 22 (2): 203–225.

Domanski, Robert J. 2015. *Who Governs the Internet? A Political Architecture*. Lanham, MD: Rowman & Littlefield.

Dunn, Myriam, and Victor Mauer. 2006. In *International CIIP Handbook 2006 – Vol. II*, by Myriam Dunn and Victor Mauer. Zurich: ETH Zurich.

ENISA (European Union Agency for Network and Information Security). 2011. *Botnets: Detection, Measurement, Disinfection & Defence*. Heraklion: ENISA Report, European Agency for Network and Information Security, 4.

Etzioni, Amitai. 2010. "Is Transparency the Best Disinfectant?" *Journal of Political Philosophy (Elsevier)* 18 (4): 389–404.

EUROPOL. 2013. *Notorius Botnet Infection 2 Million Computers Disrupted*. December 5. https://www.europol.europa.eu/content/notorious-botnet-infecting-2-million-computers-disrupted.

EUROPOL. 2015. *Botnet Takedown Through International Law Enforcement Cooperation*. February 25. https://www.europol.europa.eu/content/botnet-taken-down-through-international-law-enforcement-cooperation.

Eyal, I., and E. G. Sirer. 2014. "Majority Is Not Enough: Bitcoin Mining Is Vulnerable." In *Financial Cryptography and Data Security*, edited by N. Christin and R. Safavi-Naini, 436–454. Heidelberg: Springer.

FBI (Federal Bureau of Investigation). 2014. *GameOver Zeus Botnet Disrupted*. June 2. http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted.

FBI (Federal Bureau of Investigation). 2016. *How to Protect Your Networks from Ransomware*. Washington: FBI. Accessed December 12 2016. https://www.justice.gov/criminal-ccips/file/872771/download.

Florêncio, Dinei, and Cormac Herley. 2013. "Sex, Lies and Cyber-Crime Surveys." In *Economics of Information Security and Privacy III*, edited by Bruce Schneier, 35–53. New York: Springer.

Germano, Judith. 2014. *Cybersecurity Partnerships*. New York: The Center on Law and Security – New York University.

Grenman, Thomas. 2009. "Autoreporter – Keeping the Finnish Network Space Secure." *Enisa Quarterly Review* 5 (1): 12–14.

Hansen, Lene, and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly (Wiley)* 53 (4): 1155–1175. Accessed May 12 2016. http://www.jstor.org/stable/27735139.

Heald, David. 2010. "Varieties of Transparency." In *Transparency: The Key to Better Governance?*, edited by Christopher Hood and David Heald, 25–46. Oxford: Oxford University Press.

Hood, Christopher, and David Heald. 2010. *Transparency: The Key to Better Governance?* Oxford: Oxford University Press.

Jacobson, Douglas, and Joseph Idziorek. 2013. *Computer Security Literacy: Staying Safe in a Digital World*. Boca Raton, FL: CRC Press.

Kaspersky Lab. 2013. *What is a Botnet?* April 25. https://blog.kaspersky.com/botnet/1742/).

Kaspersky Lab. 2016. *What is a Keylogger?* 01 26. http://www.kaspersky.com/internet-security-center/definitions/keylogger.

Kharraz, Amin, William Robertson, Davide Balzarotti, Leyla Bilge, and Engin Kirda. 2015. "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks." In *Detection of Intrusions and Malware, and Vulnerability Assessment*, by Magnus Almgren, Federico Maggi, and Vincenzo Gulisano, 3–24. Heidelberg: Springer.

Lessig, Lawrence. 2006. *Code 2.0*. New York: Basic Books.

Lodge, Martin. 2014. "Regulatory Capture Recaptured." *Public Administration Review (The American Society for Public Administration)* 74 (4): 539–542.

Lodge, Martin, and Kai Wegrich. 2012. *Managing Regulation – Regulatory Analysis, Politics, and Policy*. London: Palgrave Macmillan.

McAfee. 2011. *Security 101: Attack Vectors, Part 1*. November 15. https://blogs.mcafee.com/mcafee-labs/security-101-attack-vectors-part-1/.

Microsoft. 2015. *And the Gold Medal Goes to … Finland!* June 29. Accessed June 29. http://blogs.microsoft.com/cybertrust/2014/02/20/and-the-gold-medal-goes-to-finland/.

Morgan, Bronwen, and Karen Yeung. 2007. *An introduction to Law and Regulation*. Cambridge: Cambridge University Press.

Moura, Giovane C. M., Qasim Lone, Hadi Asghari, and Michel J.G. van Eeten. 2015. *Evaluating the Impact of AbuseHUB on Botnet Mitigation – Interim Deliverable 1.0*. Delft: Dutch Ministry of Economic Affairs.

Mulgan, Richard. 2000. "Comparing Accountability in the Public and Private Sectors." *Australian Journal of Public Administration* 59 (1): 87–97.

Murray, Andrew D. 2007. *The Regulation of Cyberspace*. Abingdon: Routledge-cavendish.

Murray, Andrew D. 2016. *Information Technology Law: The Law and Society*. 3rd ed. Oxford: Oxford University Press.

Narang, Pratik, Subhajit Ray, Chittaranjan Hota, and Venkat Venkatakrishnan. 2014. "PeerShark: Detecting Peer-to-Peer Botnets by Tracking Conversations." IEEE Security & Privacy Workshops. IEEE. 108–115.

O'Connell, Jennifer. 2014. *Gameover for P2P Zeus?* June 6. Accessed March 25 2016. https://blogs.it.ox.ac.uk/oxcert/2014/06/06/gameover-for-p2p-zeus/.

Pearce, Paul, Vacha Dave, Chris Grier, Kirill Levchenko, Saikat Guha, Damon McCoy, Vern Paxson, Stefan Savage, and Geoffrey Voelker. 2014. "Characterizing Large-Scale Click Fraud in Zero Access." Scottsdale: CCS'14.

PRIPARE (PReparing Industry to Privacy-by-design by supporting its Application in REsearch) Project. 2014. "What Do We Mean by Privacy and Security-by-Design?" Accessed May 27 2016. http://pripareproject.eu/wp-content/uploads/2014/05/Privacy-and-Security-by-design.pdf.

"Russia accused of unleashing cyberwar to disable Estonia". 2007. *The Guardian*, May 17. https://www.theguardian.com/world/2007/may/17/topstories3.russia.

SANS Institute. 2001. *The OSI Model: An Overview*. SANS Institute. Accessed August 8 2016. https://www.sans.org/reading-room/whitepapers/standards/osi-model-overview-543.

Scott, Colin. 2000. "Accountability in the Regulatory State." *Journal of Law and Society* 27 (1): 38–60.

Shadowserver. 2016. *Malware*. January 28. https://www.shadowserver.org/wiki/pmwiki.php/Information/Malware.

Skjærseth, Jon Birger, Olav Schram Stokke, and Jørgen Wettestad. 2006. "Soft Law, Hard Law, and Effective Implementation of International environmental Norms." *Global Environmental Politics (Massachussets Institute of Technology)* 6 (3): 104–120.

SOPHOS. 2012. *SOPHOS Technical Paper: The ZeroAccess Botnet – Mining and Fraud for Massive Financial Gain*. SOPHOS. https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/Sophos_ZeroAccess_Botnet.pdf.

Spider.io. 2013. *Discovered: Botnet Costing Display Advertisers Over Six Million Dollars per Month*. March. http://www.spider.io/blog/2013/03/chameleon-botnet/.

Tariq, Usman, ManPyo Hong, and Kyung-suk Lhee. 2006. "A Comprehensive Categorization of DDoS Attack and DDoS Defense Techniques." In *Advanced Data Mining and Applications*, by X. Li, O.R. Zaiane and Z. Li, 1025–1036. Xi'an: Springer.

Tiirmaa-Klaar, Heli, Gassen Jan, Elmar Gerhards-Padilla, and Peter Martini. 2013. "Botnets: How to Fight the Ever-Growing Threat on a Technical Level." In *Botnets*, edited by H. Tiirmaa-Klaar, J. Gassen, E. Gerhards-Padilla and P. Martini, 41–97. London: Springer.

Tropina, Tatiana, and Cormac Callanan. 2015. *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security*. Cham: Springer.

Van Lam Le, Ian Welch, Xiaoying Gao, and Peter Komisarczuk. 2013. *Anatomy of Drive-by Download Attack*. Proceedings of the Eleventh Australasian Information Security Conference. Adelaide: AISC. 49–58.

Viestintävirasto. 2016. *CERT-FI*. 01 15. https://www.viestintavirasto.fi/en/cybersecurity/ficorasinformationsecurityservices/cert-fi.html.

Weisband, Edward, and Alnoor Ibrahim. 2007. "Introduction: Forging Global Accountabilities." In *Global Accountabilities: Participation, Pluralism, and Global Ethics*, edited by Edward Weisband and Alnoor Ibrahim, 1–23. Cambridge: Cambridge University Press.

Zittrain, Jonathan. 2008. *The Future of the Internet and How to Stop it*. Yale: Yale University Press.