Private active cyber defense and (international) cyber security—pushing the line?

Broeders, D.W.J.

JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2021, 1–14
doi: 10.1093/cybsec/tyab010
Research Paper

Research Paper

Private active cyber defense and (international) cyber security—pushing the line?

Dennis Broeders *

The Hague Program for Cyber Norms, Institute of Security and Global Affairs, Leiden University, The Hague, The Netherlands

*Correspondence address. Institute of Security and Global Affairs, Leiden University, Wijnhaven, Turfmarkt 99, 2511DP The Hague, The Netherlands. Tel: ++31 70 800 9030; E-mail: d.w.j.broeders@fgga.leidenuniv.nl

Received 3 July 2020; revised 22 February 2021; accepted 1 March 2021

Abstract

Private sector Active Cyber Defence (ACD) lies on the intersection of domestic security and international security and is a recurring subject, often under the more provocative flag of 'hack back', in the American debate about cyber security. This article looks at the theory and practice of private cyber security provision and analyses in more detail a number of recent reports and publications on ACD by Washington DC based commissions and think tanks. Many of these propose legalizing forms of active cyber defence, in which private cyber security companies would be allowed to operate beyond their own, or their clients' networks, and push beyond American law as it currently stands. Generally, public-private governance solutions for security problems have to manage a balance between (i) questions of capacity and assigning responsibilities, (ii) the political legitimacy of public–private security solutions and (iii) the mitigation of their external effects. The case of private active cyber defence reveals a strong emphasis on addressing the domestic security (and political) problem, while failing to convincingly address the international security problems. The proposals aim to create a legitimate market for active cyber defence, anchored to the state through regulation and certification as a way to balance capacity, responsibilities and domestic political legitimacy. A major problem is that even though these reports anticipate international repercussions and political pushback, against what is likely be received internationally as an escalatory and provocative policy, they offer little to mitigate it.

Key wordscybersecurity, active cyber defence, public–private governance, sovereignty, capacity

Introduction

Corporate self-help in cyberspace is a contentious issue. Even though companies suffer great costs at the hands of internationally operating cyber criminals and state sponsored actors, and governments often lack capacity and political will to provide adequate protection, companies are not allowed to take matters into their own hands. Obviously, they are allowed to construct or procure the best cyber defence of their own networks that money can buy, but they are not allowed to follow or retaliate against attackers beyond the perimeter of their own computer networks. Neither are they allowed to turn to private cyber security companies to do this on their behalf. This is grounded in national legislation—for example, the American Computer Fraud and Abuse Act (CFAA)—as well as in concerns about international security and inter-state relations, as attackers can come from anywhere on the globe, may route attacks via third countries and may turn out to be state actors. Even though the legal status quo prohibits companies from engaging in self-help or procuring help on the commercial cyber security market, the issue keeps resurfacing in the American political debate. The most extreme form, companies 'hacking back' their attackers, does not seem a viable political option but those who advocate private solutions now tend to promote the option of Active Cyber Defence, that goes beyond passive defence but stops short of hacking back (see the next section for a more elaborate explanation).

The debate about active cyber defence takes place against a background of (i) the ongoing debate about public-private

cooperation in cyber security and (ii) the wider policy and academic debates about the privatization of security. Both of these debates revolve around trade-offs between public and private capacities and the necessity of private involvement on the one hand, and fundamental considerations of responsibility and legitimacy of the resulting public–private solutions on the other. This article aims to shed light on the way the lines between private and public responsibilities in the provision of (international) cyber security are shifting and on the motivations of those that aim to shift them. It distils a framework from the literature on public–private (cyber) security governance focused on the legitimacy and effectiveness of governance solutions. Generally, public–private governance solutions for security problems have to manage a balance between (i) questions of capacity and assigning responsibilities, (ii) the political legitimacy of public–private security solutions and (iii) the mitigation of their external effects. Taking the general developments in the debate about public–private interactions and cooperation in cyber security provision as a background, this article analyses the case of recent proposals for corporate Active Cyber Defence by American commissions and think tanks in light of this framework. The USA provides the only national context in which there is a relatively open debate about these issues, and the various proposals from think tanks and commissions provide especially detailed material for the analysis. The overall conclusion of the article is that the debate on private active cyber defence reveals a strong emphasis on addressing the domestic security (and political) problem, while largely failing to address the external effects and problems of political legitimacy at the international level.

Active cyber defense: background and bandwidth

The 2018 World Economic Forum report on *Regional risks for doing business,* based on a survey of 12 548 global business leaders, put cyber-attacks at the number five spot in the global ranking of risks to doing business [1]. Among the most digitized regions and countries however, cyber-attacks were ranked first. In Europe, North America and the East Asia Pacific region and in fast growing digital economies such as India, business executives named cyber-attacks and data breaches as the dominant risk now and in the near future. Governments seem to agree. In many countries cybercrime, cyber-attacks, (economic) espionage, cyber warfare and disinformation campaigns are topping the lists of official government threat assessments, even though the empirical evidence underlying these assessments is often sketchy [2, 3]. Many governments are actively raising public awareness of cyber vulnerabilities at all levels of cyber security: individual end users, civil society organizations, critical infrastructures and private companies. On the other hand, states do not necessarily can—or want—to shoulder the burden of protecting citizens and companies in cyberspace. Capacity in law enforcement, intelligence and security agencies and the military is growing, but also seems dwarfed by the threats that governments insist are endemic and growing. Both citizens and corporations are to a large extent expected to take responsibility for their own online security [2, 4].

The mismatch between threat assessment, with both governments and corporations indicating a high risk environment, and a limited government capacity and political willingness to protect companies online, puts the spotlight on private cyber security solutions. While companies are allowed to defend their own networks, they are not allowed to retaliate or gather evidence beyond the perimeter of their own networks. However, when faced with a determined criminal, state or state-sponsored attacker, passive cyber defence often seems only part of the solution. The US government legally limits private sector defence against cyber-attacks and in the eyes of some, these limitations are too strict. For example, in the financial sector where the stakes are high and attacks are commonplace, some are advocating for a more aggressive cyber self defence posture [5, 6].

In the USA, this mix of factors has led to a periodic resurfacing of the debate on whether corporations should be legally allowed to 'hack back', or engage in more limited and less aggressive forms of Active Cyber Defence. In 2019, Robert Chesney summed it up as 'Hackback is back' in a *Lawfare* post about the proposed 'Active Cyber Defense Certainty Act' [7]. In recent years, especially Washington DC-based commissions and think tanks have been fuelling this debate by making the case for the creation of a commercial market for active cyber defence. Stopping short of advocating actual 'hack backs' (destructive counter attacks) most of them suggest that private firms should be allowed to conduct some forms of active or forward defence by operating on networks other than their own. As the majority of companies do not have such in-house capacity most proposals advise the creation of a commercial market for active cyber defence. In addition to these interventions by commissions and think tanks, a bi-partisan bill, the *Active Cyber Defense Certainty Act* (ACDC) [8], was submitted to Congress in 2017, and reintroduced in 2019, taking the debate about private active cyber defence into the heart of the American political system.

Even though the debate often takes place under the more headline worthy banner of 'hack backs', the actual proposals are usually more modest and framed as 'Active Cyber Defense' (ACD). The Center for Cyber and Homeland Security defines active defense as 'a spectrum of proactive cybersecurity measures that fall between traditional passive defense and offense' [9, p. 9]. This spectrum includes technical interactions between a defender and an attacker as well as operations that enable defenders to collect intelligence on threat actors. It also includes pure governmental policy tools such as sanctions, indictments and trade remedies that can modify the behavior of malicious actors, but the focus is mostly on what private actors can do in the digital realm itself. Much of the debate about active cyber defense is about 'the grey zone'. Under most legal regimes the boundary between legal and illegal courses of action in the face of a cyber-attack revolves around two threshold values. One is the line between operations conducted on one's own network and those conducted on another's network (either that of the adversary or that of a third party through which the attack was routed). The other threshold is the actual 'hacking back' in which adversary networks are breached, disrupted and damaged which is generally considered to be only within the remit of law enforcement. The first threshold is *within* the much debated grey zone, separating the 'light grey' from the 'dark grey', the second marks the end of that grey zone. The report by the Centre for Cyber and Homeland Security plots a number of cyber operations on a continuum between passive cyber defence and offensive cyber operations[1] (see similar figures in other reports[2,3]).

There is some variation in different reports as to what the grey zone consists of, but Fig. 1 captures its main ingredients. The lower impact/risk actions in the grey zone are generally tools of deception

1 See figure 1 in [9].

2 See similar graph in [76, p. 9].

3 See similar graph in [77, p. 4].

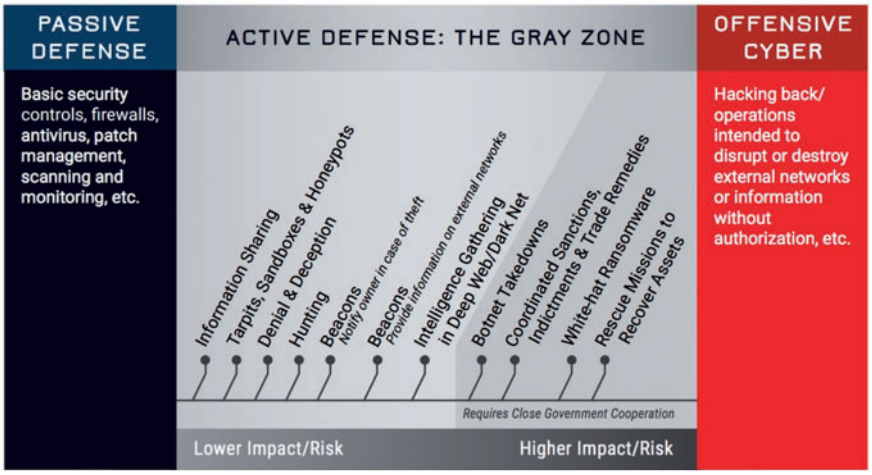

Figure 1: the continuum between defensive and offensive cyber operations.

Source: Centre for Cyber and Homeland Security [9, p. 10]

or information tools, like 'honeypots' that are embedded in the defender's network and which lure in attackers with fake attractive data, so their behaviour and methods can be studied. Many of these are legitimate cyber security measures that companies do in house or hire private cyber security companies to do for them. Sharing information and various techniques to thwart, detect and deflect attackers such as tar pits, honeypots, denial and deception techniques and hunting actively engage attackers, but on the home turf of the defender's network. These techniques are high end, but relatively common. Towards the end of the 'light grey' zone is beaconing, where measures start to operate on the network of the attacker and/or transit networks, and send information back to the home network.

Dark grey zone measures all operate outside of the defender's network and are therefore much more contested. Botnet takedowns usually require interventions on the computers of end users and the taking down of command and control servers. White hat ransomware would entail the 'use of malware to encrypt files on a third party's computer system that contains stolen information in transit to a malicious actor's system. Public-private partners then inform affected third parties that they have been compromised and are in possession of stolen property, which they must return in order to regain access to their files' [9, p. 11]. Rescue missions would be the use of hacking to infiltrate the computer networks of an adversary who has stolen information in an attempt to isolate the degree to which that information is compromised and ultimately recover it. It is clear that the darker the grey, the more intrusive the measures become, compromising the computers and systems of third parties, end users and the attacker. Given the domestic legal framework these activities are commonly understood to be illegal when undertaken by private parties. Moreover, with any of these measures there is a chance of crossing an international, jurisdictional boundary. Active cyber defense in the dark grey zone, though certainly not without precedent, is contentious and when proposals are made to allow such private operations they usually come with the disclaimer that this should be done in close cooperation with government. It is especially this part of the spectrum that would require changes in law and policy to shift the posts to allow a more active role of private companies in cyber defense, which is the focus of this article.

Irrespective of the exact proposals, the think tank and commission reports have to square a number of circles. Allowing self-help and/or the creation of a market for private ACD may perhaps solve an existing problem, but the solution will create a number of new questions and externalities that resonate with ongoing debates about the privatization of security in general and about the provision of public–private cyber security more specifically. Private, or public–private, solutions to security problems are often justified by pointing to the (government) capacity problem they seek to remedy, but the resulting shifts in responsibilities raise questions about the political *legitimacy* of the proposed solutions. Given the global nature of the internet and the fact that the more severe attacks and breaches are often the work of internationally operating cyber criminals or state (sponsored) actors, ACD may possibly affect international relations. If a company follows an attacker down the rabbit hole of the global internet there is no a priori telling in which country and jurisdiction it is going to resurface. If private parties conduct disruptive 'dark grey' operations on foreign, perhaps even state operated or affiliated networks, this can easily have an escalatory effect as foreign actors are likely, and may even be keen, to take offense. Especially in the current times of heightened geopolitical tensions some states will not look kindly on private companies that are legally licensed by the American government to conduct intrusive and disruptive cyber operations.

Private cyber security solutions: balancing capacity, responsibility, legitimacy and external effects

Private, or public–private, solutions to security problems are nothing new and have resulted in new national and international governance arrangements in many fields of security. Especially since neoliberalism took hold in the 1980s, favouring market solutions over 'cumbersome state solutions', private companies took up security roles that were traditionally regarded state responsibilities. Domestically, private companies moved into areas such as protection and surveillance, the prison system, secure transports and private policing of semi-public spaces such as malls and gated communities. Internationally, the privatization of security similarly took many forms. Security companies such as G4S, providing security personnel, monitoring equipment, response units and prison transports, became globally operating powerhouses with branches on every continent [10, 11]. For a while, private military and security

companies (PMSCs) were effectively and openly operating as modern day mercenaries [12, 13]. Now they have distanced themselves from the label of mercenaries but are still an almost integral part of US military deployment as private contractors providing non-combat services—although the line is often thin. They also provide commercial shipping with protection against piracy in dangerous international waters such as the Gulf of Aden [14].

Crucially, cyber security is to a large extent a privately traded commodity [15, 16], something that end users—private, governmental and corporate—have to arrange for themselves. The growth of the internet saw a growth of the private cyber security market, diversifying into different aspects of cyber security from low-end consumer security to high-end national security. Similarly, the relationship of states to the internet changed from 'benign neglect' to one of profound (security) interest as the internet grew into an important pillar of state economies and societies [17–19]. With that the security questions became quantitatively and qualitatively more significant—introducing high-end cybercrime, digital espionage and cyber operations by states.

The public–private dimension of the provision of security on the internet is characterized by private ownership of critical infrastructures and—at least initially—a capacity gap between the public and the private sector. The state itself depends heavily on cyber security companies for its own security needs. This ranges from very mundane security (firewalls, anti-virus software) via much more refined operational and forensic needs, to high end security needs in intelligence and military affairs [20–22]. Providing security as a public good for end users and companies is also layered, ranging from security provisions that are clearly a private responsibility—such as adequate defensive cyber security of corporate networks—to the protection of citizens and companies in cyberspace through law enforcement or even military protection, which are traditionally state tasks. That leaves a substantial section in the middle where public–private approaches are common. Active cyber defence is at the controversial upper end of that middle. More generally, however, most national and international cyber security policies carry the expectation that public–private cooperation is an inevitable part of effective cyber security governance. Many studies have looked at different aspects of public–private security cooperation in cyberspace [2, 4, 23–26].

The academic literature on public and private security provision suggests that all public–private governance solutions to security problems have to take into account that a number of interests, opportunities and restrictions have to be balanced. All governance solutions need to manage a balance between (i) questions of capacity and assigning responsibilities, (ii) the political legitimacy of public–private cyber security solutions, and (iii) the mitigation of their external effects.

Responsibility and capacity

A prime question is who is *responsible* for (cyber) security? With the exception of the ends of the security spectrum, the answer is often that the responsibility is shared between public and private parties, but that the demarcation of the respective roles is difficult and shifting. In criminological literature the 'pluralisation of policing' is studied by some as an empirical phenomenon [27], while others depart from the normative notion that the state is the only legitimate actor in security provision [28]. The latter school argues that the state should *anchor* the increasing plurality of security actors in order to safeguard the public interest [29, p. 93]. In doing so, it asserts the central authority of the state [30, p. 411]. This does allow some degree of pluralism in security provision as long as it is tied to and orchestrated by the state, and therefore legitimized by the state. Responsibility in this respect is already tied to larger notions of political legitimacy.

A more pragmatic reason to assign responsibility is based on the question: who is best equipped to deal with this problem? Central to this pragmatic approach is the matter of capacity, which features prominently in discussions about cyber security provision. Both in terms of information needed for threat assessment as well as in terms of capacity to defend and respond to attacks the private sector is often thought to be ahead of government defenders. Much of the relevant data, knowledge, expertise and operational know-how resides with private companies, supporting the idea of public-private solutions. As Madeline Carr argues, this need for public–private cooperation often obfuscates the fact that the challenge and the threats are not the same for the public and the private sector: 'the private sector regards cyber-security challenges as financial and reputational—not as a common public good, which is how governments regard national cyber security' [2, p. 55]. If the goals do not (fully) align it is also difficult to assign responsibilities effectively. That starts at the basic level of information sharing. Governments require information on breaches and attacks from companies but these often do not see the gain of increased transparency as it may expose their vulnerability and tarnish reputations. The resulting lack of reliable data on threats and incidents both at corporate and state level are problematic for policy making and for research [2, 31, 32].

Sometimes, lack of government capacity and inability to directly intervene on the relevant networks results in a situation where governments effectively execute their policies through private companies. Government may 'deputise' companies or infrastructural parties such as ISPs to execute certain policies for them through what David Garland calls 'responsibilisation' [33] or what Benoit Dupont calls 'third party policing' [34]. Sometimes this means that companies get responsibilities thrust on them they do not seek—like content control and censorship—but in other cases companies are keen to step into a developing security market. Adam White underscores that both public and private actors have a high degree of political agency and that the behaviour of private security actors is structured by shifts in supply and demand of security [29, 30, 35, p. 413]. It is not just a lack of government supply of security—i.e. a government supply deficit that needs to be filled by private security companies—but the deficit can also be caused by an escalation of *demand* for security [29, p. 87]. For those companies that want to develop new cyber security markets it makes political sense to reconcile their activities with notions of the public good if it contributes to their legitimacy as security actors [29, p. 97]. However, as Madeline Carr has noted, private business interest do not necessarily and always align with the public good, making scrutiny of the public credentials of private companies necessary.

Political legitimacy

The political legitimacy of private and public–private cyber security solutions is often built on fundamental political notions of sovereignty on the one hand and on pragmatic notions of effectiveness on the other. Fritz Scharpf in the context of democratic policy making, distinguished *input legitimacy*, those affected by collectively binding decisions should have a say in the decision-making process, from *output legitimacy*, which refers to the effectiveness of policies in the sense that they serve the common good [36, 37]. It is easy to see how private cyber security capacity and public–private solutions can contribute to output legitimacy by increasing the availability of

effective and readily available security solutions. This holds especially true if it is shaped in such a way that that private actors are acting as 'delegates' of public authority or otherwise operate in the 'shadow of hierarchy' [38, 39].

While output can boost the legitimacy of private security provision, the more fundamental challenge to legitimacy comes from the notion of state sovereignty and its relationship with the provision of security. Input legitimacy requires solutions to do justice to their organizing principles: democratic decisions cannot be made without the input of the people. In the case of cyber security provision, 'sovereignty' functions as its anchoring principle and provides the input legitimacy. The claim to the monopoly on the legitimate use of force has become a cornerstone of domestic state sovereignty [40, 41]. Security came to be regarded as a public good that should be provided by the government, effectively delegitimizing the use of force by other, private, parties. Even though the monopoly on the legitimate use of force is historically a relatively new constitutive element of modern state formation, its symbolic power cannot be underestimated. For example, Lucas Kello points out that in the digital age states face a 'sovereignty gap'. One manifestation of that is that the private sector can 'no longer take for granted the ability of the government to protect it against all relevant threats' [42, p. 229]. Domestic, Weberian sovereignty has an international counterpart in the notion of Westphalian sovereignty that holds that states are the only legitimate security actors in the international domain.[4] Internationally, state sovereignty is also often seen as the input legitimacy to (cyber) security solutions. Some authors try to fold the internet into the Westphalian model of international politics [42, 44, 45] and states like Russia and China are actively advocating notions of cyber sovereignty as the organizing principle of international relations in cyberspace [46–49]. Although sovereignty is not a very precise concept—Stephen Krasner famously referred to sovereignty as 'organized hypocrisy' [50]—or even a good fit with cyberspace [51] it is a concept that plays a pivotal role in determining the legitimacy of governance solutions for security problems. Weberian internal sovereignty and the Westphalian external sovereignty are—and always have been—more theoretical ideal types than reality, but do inform important notions about the legitimacy of the state and its role in the provision of domestic and international security. Scholarly debates about the privatization of security are often informed by the notion that the provision of security *ought* to be a public good: it serves as a critical benchmark for evaluating the role of public and private actors in the field of (cyber) security.

External effects

The legitimacy question at the international level is also bound up with more 'practical aspects' of international security. Allowing private (cyber) security companies to operate internationally carries the risk of legal and practical security consequences. The legal aspects are manifold but two aspects stand out. The first is the question whether the kind of activities private parties employ, would reach the level of the international legal prohibitions of 'mercenarism'. Given the fact that active cyber defence is situated in the grey zone, below the level of hack backs, this seems an unlikely possibility, although not necessarily in terms of *political* framing by a disgruntled adversary. Secondly, private cyber security companies operating across borders are likely to touch on the international debate on if and how cyber operations conducted by states or their proxies, are in violation of principles of international law such as sovereignty and the principle of non-intervention. The Tallinn manual 2.0 deals with cyber operations by non-state actors under the chapter heading 'Cyber operations not *per se* regulated by international law', making the general principle very clear [52, pp. 174–76, emphasis in original]. Even though there are some limited cases in which international law addresses non-state actors '(. . .) by and large (it) does not regulate cyber operations conducted by non-State actors, such as private individuals or companies' [52, p. 175; 53]. However, in the current situation of 'unpeace' [42] especially western states are increasingly trying to impose consequences on the actors that conduct malicious cyber operations. State are pushing back against cyber operations suspected to be carried out by states or their proxies through public attributions and even attribution coalitions [54, 55] and are taking cautious steps in the direction of calling them out in terms of international law [56]. Even though this debate focuses on international law and, therefore state behaviour, the role of proxy actors in cyber-attacks that are below the 'threshold of the use of force' is prominent [21]. This brings the behaviour of non-state actors into the legal mix, although the evidentiary requirements to prove that proxies are indeed working on behalf of state are often difficult to meet [57]. Moreover, any private operations taking place on networks and servers in another country are likely to in breach of local domestic criminal law. Given the current geopolitical strife in cyberspace, private companies engaging in active cyber defence, either as self-help or commercially on behalf of others, may well find themselves in a hostile international environment and could be easily framed as state proxies.

At a more practical political level private ACD carries a risk of escalation that goes beyond the legal domain. Even when cyber operations are 'below the threshold' and/or when states do not invoke international law to call them out, tensions between states can be ignited or exacerbated by private companies crossing digital borders and jurisdictions. Especially when their actions are perceived as disruptive and offensive, for example when private firms would reach into attacker's networks to gather forensic evidence or to retrieve or destroy (the stolen) data. The transnational actions of private companies can inadvertently escalate a conflict between states, or even be (mis)used for escalation. It may certainly add to the dynamics that Ben Buchanan discussed under the flag of the cyber security dilemma [58]. James Lewis, of the Center for Strategic and International Studies, calls hacking back 'a remarkably bad idea that would harm the national interest'. Moreover, he says that 'encouraging corporations' to compete with the Russian mafia or Chinese military hackers to see 'who can go further in violating the law, is not a contest American companies can win' [59]. Even though only state operations could be a violation of another state's sovereignty, private self-defense practices can seriously damage a state's foreign policy, by provoking collateral damage and trigger escalation of back-and-forth private attacks [60].

Any proposal for a private or a public–private solution for Active Cyber Defence would need to provide a convincing arrangement of these different questions of capacity and legitimacy, taking into account that they are playing simultaneously on a domestic and an international political chess board.

Active cyber defence: practice and ambiguity

The current legal framework does not leave much room to manoeuvre. In the case of the USA, Chris Cook points to the Computer Fraud and Abuse Act (CFAA), the Wiretap Act, The Electronic

4 Although this is to a large extent a foundational myth of IR, see [43].

Communications Privacy Act (ECPA) and the federal prohibition on Pen Register Track and Trace (PRTT) devices as statutes that 'in some form prohibit unauthorised access and/or collecting or intercepting data on a system outside of one's own' [61, p. 211]. Even though hacks backs are forbidden in the USA, government officials, and especially ex-government officials have alluded to the practice and the idea of active cyber defence in neutral or supportive terms. General Hayden, former director of the NSA as well as the CIA, was fairly blunt about it in a panel discussion at the Aspen Security Forum in 2011, stating: 'Let me really throw out a bumper sticker for you: how about a digital Blackwater?' I mean, we have privatized certain defense activities, even in physical space, and now you've got a new domain in which we don't have any paths trampled down in the forest in terms of what it is we expect the government—or will allow the government—to do' [62].

There are already private companies operating in the 'grey zone' of active cyber defense. As indicated before, some activities in the light grey zone—such as tarpits and honeypots, denial and deception, and beaconing on your own network—are mostly a normal part of the portfolio of specialized cyber security companies that set up sophisticated cyber security for high-end customers or come in after a successful cyber-attack for forensic analysis. Private cyber security companies are also active in the attribution of high end cyberattacks to specific groups and sometimes even point the finger towards states and state actors. Many attributions of state sponsored cyberattacks were originally and in some case predominantly the work of private cyber security companies, exposing and naming some of the most notorious APTs, although the overall view of the threat landscape that results is biased towards high-end threats to high-profile victims [63]. While these forensic activities and attributions (mostly) do not venture into third party networks, they do venture into the realm of international cyber security (geo)politics as states sometimes build on these reports to (publicly) call out malicious state actors.

In specific cases private companies, whether or not in concert with the American government, have also ventured into the dark grey zone of active cyber defence. Healey, Jenkins and Work [64] have been building a data set of what they call 'defensive operational disruption' which seems to correspond well to the dark grey zone. They look at disruptive counter-cyber operations that are typically done outside of the defender's own network or based on specific intelligence on how that adversary operates [64, p. 253]. These operations can be done by governments, cyber security or technology companies or the victims of an attack. Their dataset highlights a substantial number of operations that are led by industry or by public–private partnerships and use intrusive techniques such as white worms, takedowns of bullet proof hosting, disclosure of APTs and (many) botnet takedowns. Botnet takedowns by private corporations, that identify and disconnect zombie computers from the command and control infrastructure, are increasingly common, if not always unproblematic. Between 2010 and 2014 Microsoft successfully took down at least nine botnets, but also took up to five million unrelated websites off line as collateral damage [34, pp. 104–7]. According to Benoit Dupont these highlight '(. . .) the structural mismatch between highly resourced transnational corporations and national court systems that lack the capacity to supervise the results of technically complex decisions, whose ramifications are not always well or fully understood' [34, p. 107]. Other schemes follow a model of polycentric regulation of botnets in which countries have placed ISPs and anti-virus companies at the heart of take down operations, instead of the police or a single multinational corporation [65, 66]. Intrusions into the attacker's networks with a view to recovering stolen data and/or gathering forensic evidence have also happened. One famous case is that of *operation Aurora* in which Google counterattacked against a China-based advanced persistent threat group that was reportedly after both e-mail accounts of Chinese dissidents as well as Google source code. In this case, Google broke into the servers of the attackers, gathered intelligence about the attack and the attackers and then shared the information with the American government. This case became part of a much wider geopolitical process in US–Sino relations in cyberspace [22, pp. 171–86; 67] but it is important to note that this specific public-private partnership was constructed *after* Google hacked into its attackers' servers, making Google's actions a gamble that paid off.

In addition to cases such as these that became part of the public domain, companies themselves have indicated that they want more leeway in dealing with attacks. At the 2015 meeting of the World Economic Forum in Davos the banking industry debated the issue. Especially American banks were in favour of a more aggressive approach to cybercrime and attacks, with one bank's head of technology claiming that 'finding and immobilising the command and control servers of attackers should be "well within our rights"' [5]. In 2014, Ellen Richey, Visa's vice chairman for risk and public policy, concluded in this context that 'The primary thing the government can do, is number one, get out of the way' [cited in 6, p. 108]. Although statistics are scarce, anecdotal evidence suggests that private companies are at times retaliating against cyber attackers. An often quoted survey conducted at the Black Hat USA security conference in 2012 indicated that 36 percent of 181 surveyed companies had at least once engaged in retaliatory hacking [68]. In 2018 Tom Fanning, CEO of Southern Co., stated at a public event of the Aspen institute: 'If hackers hit the US power grid, they'll be hit right back', leaving some room to wonder whether the response would be by the company, the American military or the two of them in tandem [69]. Tom Kellerman, chief cyber security officer for Trend Micro and a former member of President Obama's commission on cyber security said that 'Active defence is happening. It's not mainstream. It's very selective', before adding that he and his company would never do it [68]. Government officials also acknowledge that the practice exists in spite of legislation prohibiting it. Statements range from clear cut public condemnation of 'strike back techniques of any kind by firms or other private actors' by Assistant Attorney General Leslie Caldwell in 2015 to more ambiguous statements such as that by NSA director Admiral Mike Rogers who surmised that though he was not a 'big fan of the idea, it is not without precedence' [cited in 42, p. 236].

The grey zone is not unchartered territory, but is also not in the open making the scale and scope of private activities unclear. Those who go into the details of what active cyber defence may entail will have to weigh the possibilities against questions of capacity and legitimacy, and the domestic and international political external effects identified before.

Talking active defence to power: think tanks and other advisors

In recent years, the debate about active cyber defence has been fed by a number of reports and policy briefs coming out of Washington DC think tanks and commissions. On the issue of ACD a number of think tanks and commissions have brought out reports and other think pieces, although of the 'DC-5' [70, p. 9], the largest and wealthiest of the DC think tanks, only the American Enterprise Institute is represented. Seven relevant reports were identified, as

Table 1: overview of the documents analysed

Year	Authors	Background authors	Organization	Political character	Product
Commissions and think tank reports					
2013	The Commission on the Theft of American Intellectual Property	Former government (including national security) and business	The Commission on the Theft of American Intellectual Property	Bi-partisan, independent commission	Report
2013	Irving Lachow	Researcher	Centre for New American Security (CNAS)	Bi-partisan think tank on national security	Policy brief
2015	Juan Zarate	Former government (national security)	Foundation for Defence of Democracies	Non-partisan, but also described as 'hawkish' and 'neo-conservative' [71]	Report
2016	Ariel Rabkin and Jeremy Rabkin	Researchers	American Enterprise Institute	Non-partisan, but also described as (neo)conservative	Policy Working paper
2016	Centre for Cyber and Homeland security—task force	Former government (incl. national security), business and academia	Center for Cyber and Homeland security (GW University)	Taskforce is non-partisan	Project Report
2017	Wyatt Hoffman and Ariel Levite	Researchers	Carnegie Endowment for International Peace	Non-partisan	Report
2017	Paul Rosenzweig, Steven Bucci and David Inserra	Former government (national security) and researchers	The Heritage Foundation	Conservative	Backgrounder
Legislation					
2017	H.R. 4036 (Active Cyber Defense Certainty Act) Submitted to Congress by Tom Graves (R) and Kyrsten Sinema (D) Re-submitted in 2019 as H.R.3270 (Active Cyber Defense Certainty Act)				

well as the bi-partisan Active Cyber Defense Certainty Act submitted to Congress, and will be used to go into the specifics of what it could mean to legally condone or stimulate active cyber defence and if and how these reports address the balancing act between capacity and legitimacy. Table 1 gives an overview of, and some background on, these reports and papers.

The products that these think tanks and commissions delivered vary from official reports to working papers, meaning that the political weight and institutional backing differs as well. Most of the reports have been prepared by, or for, neutral or bi-partisan think tanks or commissions, but a number of these can be characterized as politically (neo-) conservative. Some reports have been written by think tank staffers, but many have been (co-)written or chaired by former government officials, often with a background in national security (homeland security, the military, intelligence agencies, national security advisors) from both democratic and republican administrations. The Centre for Homeland Security task force for example, was chaired by four co-chairs from former intelligence, former government and an NGO. Moreover, the taskforce had a wide membership with representatives from government, NGOs, academia, think tanks and (tech) corporations.

In terms of what these organizations and authors understand ACD to be, there is a difference between their *analytical* take on what measures they consider to be part of the grey zone of ACD—as discussed in this article in section 'Active cyber defence: background and bandwidth' '—and their *recommendations* to government as to what is and should be allowed under the heading of ACD. In general, the reports tend to be much clearer and specific on the first than on the second. However, it is the policy recommendations, and solutions to deal with the caveats of those proposals, that are of interest for this article. Therefore, Table 2 summarizes per report (i) which ACD measures are explicitly mentioned with a view to legalizing them, and (ii) what kind of scheme, if any, is proposed to legitimize private ACD (usually some form of certification).

This gives an overview—at a high level of abstraction—of the main thrust of the recommendations in the reports. One main takeaway from this table is the fact that many of the reports tend to be relatively unspecific in their recommendations, especially when it comes to the dark grey measures. Many do not explicitly name *which* measures in the dark grey zone should be given a legal basis, but rather signal the problem in general terms and call upon government to legislate and certify (and hence be more specific).

The devil is in the detail: an in-depth analysis of the proposals

Capacity and responsibility

Many of the reports take the problem of capacity as their point of departure, stressing that cyber threats are on the rise and that the government lacks the capability to deal with those threats. Some add to this the argument that the private sector *does* have these capabilities. Allocating responsibilities to private parties is firstly addressed through the legal framework, which needs clarification but mostly needs to be expanded to legitimately assign new roles and responsibilities.

Most reports point to rising threat levels as the main rationale for the need to (re)think ACD. In the words of the Centre for Cyber and Homeland Security: 'Simply put, threats are expanding in

Table 2: proposed ACD measures and legitimization by government

Organization and authors	Understanding of private active cyber defence and the government's role
The Commission on the Theft of American Intellectual Property (2013)	The IP Commission gives a general recommendation to the government to legalize parts of the grey zone. Explicit mentions of 'beaconing' and 'white hat ransomware' that should be considered legal.
Centre for New American Security (Irving Lachow, 2013)	Lachow merely identifies a grey zone between 'ACD measures within [a company's] own networks and systems', which is legal, and 'any actions that destroy data on or cause harm to the C2 server or other computers outside of a company' that are almost certainly illegal. Measures in the grey zone require 'further guidance'.
Foundation for Defence of Democracies (Juan Zarate, 2015)	Zarate: Government can facilitate information security by eliminating corporate liability and can 'freeze assets and block transactions against those (. . .) identified as being behind major cyber infiltrations, disruptions, and espionage'. Also, government can create 'special cyber warrants'—another type of 'letter of marque and reprisal'—to allow US private sector actors to track and even 'hack back' or disrupt cyberattacks in certain instances to defend their systems.
American Enterprise Institute (Ariel Rabkin and Jeremy Rabkin, 2016)	Rabkin and Rabkin promote private 'countermeasures', which lie between passive defence and strategic (military) intervention, but only outside of the jurisdiction of the USA and friendly powers. Measures should 'not involve physical injury to persons or extensive damage to private property'. 'The government should regulate who performs hack-back, supervise the targets for such action, and regulate the means'.
Center for Cyber and Homeland security (2016)	Hack backs and rescue missions of stolen data 'should continue to be prohibited'. The government should reassess legislation to ensure that 'low and medium-risk active defense measures are not directly prohibited in statute' nor 'prioritize [them] for investigation or prosecution'. Government could 'grant licenses to certain cybersecurity companies that would allow them to engage in limited active defense techniques'
Carnegie Endowment for International Peace (Wyatt Hoffman and Ariel Levite, 2017)	Other than excluding 'hack backs', Wyatt and Levite do not specify what should and should not be allowed: '(. . .) rather than trying to enforce ineffectual laws and regulations, governments and stakeholders should seek to develop guiding principles for a spectrum of ACD'.
The Heritage Foundation (Paul Rosenzweig, Steven Bucci and David Inserra, 2017)	Use the language of 'annoyance—attribution—attack'. Annoyance (light grey) tactics such as information sharing, denial and deception and hunting are allowed under US law. More problematic 'attribution' activities such as beaconing and dark web information gathering, should be allowed to private parties which are certified by government.
Active Cyber Defense Certainty Act (2017)	ACD explicitly allows 'beaconing' and wants the government to refrain from criminal prosecution of active cyber defence (entering network of the attacker) in order to (i) establish attribution, (ii) disrupt ongoing attack and (iii) monitor attackers' behaviour. Under conditions of not being reckless. Intentional access to an intermediary network is not allowed The FBI must set up a program for pre-emptive review of ACD. FBI must be notified and must respond (acknowledge receipt) of an active defence measure

persistence and consequence and we cannot solely rely on defensive measures and "firewall" our way out of this problem' [9, p. v]. Cybercrime is often mentioned, but many also point towards the rising threats of sophisticated state-enacted or sponsored hacks in the form of Advanced Persistent Threats (APTs) [72, pp. 1–3; 9, p. 6; 73, p. 11]. By pointing towards state actors as some of the main threats the framing becomes more geopolitical and urgent. Juan Zarate, writing for the Foundation for the Defence of Democracies, with a specific focus on the financial system, maintains that 'Western banks and the financial system are now encountering the convergence between economic and cyber warfare' [73, p. 5]. Also drawing attention to the blurring of the boundary between the corporate and the geopolitical world, the Centre for Cyber and Homeland Security writes: 'Businesses never anticipated the scale to which they would be responsible for defending their interests against the military and intelligence services of foreign countries' [9, p. 3]. The IP Commission underscores that cyber enabled theft of intellectual property, especially by state actors, links corporate interests with national interests [74]. The closer the link between national security and corporate security—for example, in case of the financial system as a critical infrastructure—the more urgently the call for action is formulated, for example by Zarate: 'This would also entail a more aggressive "cyberprivateering" model to empower and enlist the private sector to better defend its systems in coordination with the government' [73, p. 6].

The threat landscape is then used to call into question the government's capabilities to deal with those threats on behalf of the private sector. The Center for Cyber and Homeland Security draws attention to the particularity of the threat: 'One key aspect that differentiates cybersecurity threats from other security threats is the extent to which the government appears unable to adequately protect the private sector' [9, p. 3]. Senator Graves, one of the sponsors of the Active Cyber Defense Certainty Act, also pointed to a lack of government capacity as the underlying rationale for the act [75]. Others, such as Hoffman and Levite writing for the Carnegie Endowment, stress both a lack of resources and political will: 'Most governments are becoming unable and *unwilling* to protect citizens and private enterprises against numerous, sophisticated cyber predators seeking to disrupt, manipulate, or destroy their digital equities' [76, p. 1, emphasis added].

The other side of the coin of a presumed lack of government capability is the presumption that the private sector does have the capability to deal with these threats (but is held back by the current legal framework). Rosenzweig et al. [77, p. 3], writing for the Heritage Foundation, and the Center for Cyber and Homeland Security [9, p. 25] stress that capacity is available in the private sector, while other advisors, most notably Rabkin and Rabkin [78, p. 11], writing for the American Enterprise Institute, have a more neoliberal line of reasoning that private solutions are inherently better and that 'the market can do the sorting'. The overall sense that the government cannot deliver, and stands in the way of private companies defending themselves, also acquires a moral component for those in favour of a more aggressive approach: 'In the absence of an effective system of cybersecurity provided by the government, it is in some sense immoral to prohibit private-sector actors from protecting themselves' [77, p. 11]. In summary, the reports mostly align in their analysis of the problem, i.e. a rising threat that takes on elements of national security, and a private solution that is waiting in the wings but needs to be liberated from legal restraints.

Most of the reports argue that the legal framework in the USA stands in the way of active cyber defence. As long as the legal framework is unclear or too restrictive there is no solid basis for reallocating roles and responsibilities, even in a situation where there is capacity available in the private sector. Most conclude that the current domestic legal framework is either ambiguous, or just clearly prohibits corporate self-defense. The Center for Cyber and Homeland Security on the basis of their legal analysis concludes: 'What is clear is that under U.S. law, **there is no explicit right to self-defense** ("self-help") by private companies against cyber threat actors' [9, p. 17, emphasis in original]. The transnational character of the internet (and of cyber-attacks) means that at the very least the domestic laws of other countries are part of the equation. Whether that clinches the argument is another matter. On the issue of international law Rabkin and Rabkin [78, p. 14] cite an earlier article by Paul Rosenzweig who 'After posing the question of whether international law is relevant to debates about "private sector hack back"', answered, as a 'fair, first approximation answer': 'no, it isn't. Not at all' [79]. In 2017, Rosenzweig et al., writing under the flag of the Heritage Foundation, roughly stands by that assertion, arguing that as existing international instruments do not mention private-sector offensive cyber activity anywhere and, 'more fundamentally, with very limited exceptions, international law is directed at nation-state actors and is intended to control their behavior' [77, pp. 6–7]. Even so, one of their main conclusions still reads 'To the extent that any customary international law exists at all, it is likely to discourage private sector self-help outside the framework of state authorized action' [77, p. 3]. The nod towards 'state authorization' already indicates that they see possibilities for a scheme that anchors private capacity to public legitimacy. The overall conclusion of the reports and commissions is that the legal framework (i) needs to be clarified, especially when it comes to the light grey zone of ACD, and/or (ii) needs to be adapted to make the more intrusive levels of ACD legally possible.

The report of the Centre for Cyber and Homeland Security is entitled 'Into the Gray Zone', indicating that the legal framework for some of the measures under the umbrella of ACD is unclear. Other reports agree with that assessment. Hoffman and Levite, writing for the Carnegie Endowment, say that US domestic law is 'ambiguous or even amorphous regarding the permissibility of ACD short of extreme cases' [76, p. 17]. Similarly, Lachow, writing for the Center for New American Security, maintains that the ends of the spectrum are almost certainly allowed and forbidden respectively, but work is needed from policy makers on clarifying the 'grey zone' [72, p. 8]. A logical first step for most of the reports is to clarify the existing law and mark out what is and isn't legal under the current framework: 'The U.S. government needs to provide greater clarity on which ACD actions are legal and which ones are not' [72, p. 10]. In Lachow's view, this is important because otherwise 'organizations may choose not to take actions that are legal because of fears of breaking vague provisions of existing law' or, conversely, 'organizations may take actions that they believe are legal but that government authorities view as being illegal'. Rosenzweig et al. maintain that 'Congress and the Administration should make clear that low-risk active defense techniques such as information sharing, denial and deception, and hunting activities are permitted under U.S. law' [77, pp. 10-11]. The Center for Cyber and Homeland Security calls for the government to eliminate 'the legal "gray areas" by calling on the Department of Justice to make clear which 'active defense measures it interprets to be allowable under current law, indicating that DOJ would not pursue criminal or civil action for such measures assuming that they are related to the security of a company's own information and systems' [9, p. xii]. Here clarification of the law also dovetails with issues of liability and (non-)prosecution of companies that engage in ACD, something that is high on the lists of many advisors when it comes to changing the legal framework. Most of the reports are in agreement that clarification of the legal framework is the low hanging fruit. The combination of explicitly sanctioning what is allowed, in some cases in combination with appeals to guarantee non-liability, are easy routes to improve corporate cyber defense. These lighter shades of grey are however not the reasons the debate about ACD is so contested. To truly make a dent in the problem, most of the reports call for a new legal framework to make room for self-help and for the regulation of a commercial market for active cyber defense.

The Center for Cyber and Homeland Security simply states: 'There is a need for government to partner with the private sector in developing and implementing a framework for active defense' [9, p. v]. Some target specific laws, such as the CFAA [9, p. xiii], while others, such as the IP Commission, highlight the overall need to level the playing field between the attackers and those under attack:

> (. . .) new laws might be considered for corporations and individuals to protect themselves in an environment where law enforcement is very limited. (. . .) Informed deliberations over whether corporations and individuals should be legally able to conduct threat-based deterrence operations against network intrusion, without doing undue harm to an attacker or to innocent third parties, ought to be undertaken [74, p. 82].

Most reports, conscious of the link between security and sovereignty, are eager to argue that their proposals for a more active security role for private companies is anchored to state sovereignty as a source of legitimacy. Hoffman and Levite state that: 'Allowing a certain level of private sector engagement in ACD does not necessarily entail an irrevocable loss of state authority' [76, p. 42]. Safeguarding legitimacy at the domestic level clearly entails reconciling private ACD with Weberian state sovereignty. The reports highlight three major ways of doing just that. The first is plain and simple legislation. Especially for the lower levels of ACD the reports envision that it should be enough to explicitly allow some private actions under a new legal framework. The second is to regulate and legitimize a market for private active cyber defense solutions. The main instrument for doing that is through some form of certification by the government. The third seeks to remedy the problem of capacity through what effectively is the deputation of private

companies. High end ACD can only be done by technically advanced private actors in (close) cooperation with law enforcement, connecting private technological capacity to public state legitimacy. However, even though this may cover the domestic political legitimacy of the scheme, it does not necessarily address international security concerns. International law enforcement is characterized by (often cumbersome) cooperation between states and not by unilateralism. Most of the proposed legal changes are however quite vague on the what—i.e. what would be allowed—and relay their focus on the how and the who: *who* should be allowed to engage in ACD and *how* can that be legally and politically justified. Much of the debate is about various schemes of certification, while it remains relatively unclear *what* should be certified.

The regulation of a commercial market for ACD is the preferred way to bring capacity in balance with responsibilities. The legal framework paves the way for new private responsibilities and the availability of commercial solutions to more serious cyber security problems would increase the *output legitimacy* of the change in the governance of cyber security provision. Certification and other suggestions that require the government to sanction and approve private ACD solutions are meant to 'anchor' the market—although in some cases quite lightly—to the state in an effort to increase the *input legitimacy* of the proposals.

There is anecdotal evidence that some companies already provide ACD services but this 'market' operates under the radar and there is no reliable estimation of how big the phenomenon might be. Reputable cyber security companies do not wish to be associated with hack back practices as evidenced by Mandiant's reaction to David Sanger's claim that the company 'reached back' through the networks of the Chinese APT1 group [80, pp. 101–2; 69]. In a blog post, the company responded to this claim by saying: 'To state this unequivocally, Mandiant did not employ "hack back" techniques as part of our investigation of APT1, does not "hack back" in our incident response practice, and does not endorse the practice of "hacking back"' [81]. Companies such as Mandiant do not wish to operate in the (outer reaches of the) grey zone under the current legal regime and may also reject the practice on its own merits, irrespective of the legal framework. The latter is hard to say given the legal status quo. However, when the reports talk about regulating a market and certification they often think of companies like Mandiant.

The various proposals for certification schemes differ in how strict companies should be regulated and also in what need the certification should address. Certification is sometimes meant to assure the level of technological sophistication needed to engage in ACD—and thus sees to the quality of capacity—and sometimes to create a link of legitimacy with government oversight, although these are obviously not mutually exclusive. Rabkin and Rabkin propose a three-pronged regulatory regime: 'the government should regulate who performs hack-back, supervise the targets for such action, and regulate the means' [78, p. 11]. The certification regime that goes along with it seems rather light though. They call on the Department of Justice to keep a list of companies authorized '(. . .) to do such work, with membership revoked for carelessness or recklessness' [78, p. 11]. Hoffman and Levite advocate self-regulation but also open the door for government regulation. One option would be 'registration, certification or accreditation', another would be for the government to 'deputize, on a selective basis, those wishing to engage in ACD (. . .), as was occasionally done in other domains where governments by themselves proved unable to impose law and order' [76, p. 73]. Rosenzweig et al. assert that higher levels ACD ('more aggressive and legally problematic "attribution" activity') should be legally allowed to private parties that are certified by the Department of Homeland Security [77, pp. 10–11]. These could be outside market parties but also in-house departments in the case of bigger corporations. Their proposed certification scheme requires DHS to cooperate with the National Institute of Standards and Technology (NIST) to assess the technical proficiency of those that wish to be certified. The Center for Cyber and Homeland Security also underlines the importance of certifying technological capacity and skills [9, p. xiii], but additionally suggests a licensing strategy [9, pp. 28–29]. Finally, the draft legislation of the ACDC indicates that defenders should be 'qualified defenders' but does not specify a qualification and certification mechanism. Instead, it sketches a mechanism that requires that all active defence *measures* must be notified to the FBI and that this notification must be acknowledged before actually taking active measures. Not so much a certification of actors but a vetting—and approval—of proposed private actions by law enforcement. Most of the certification schemes seem relatively light touch. They aim to increase output legitimacy (certifying the *quality* of defenders) as well as input legitimacy (bestowing state legitimacy on private solutions). They are however, mostly anchored to *domestic* agencies of law enforcement, leaving questions on the legitimacy of these solutions in the international domain largely unanswered.

Piracy, both contemporary and of bygone centuries, serves as an inspiration for some of the proposed certification schemes. In the age of privateering, which ended in the 19th century, private vessels could be licensed by government to attack a hostile government's trade. In peacetime private ships could under the concept of 'reprise' raid another nation's commercial ships at sea to compensate for losses suffered at the hand of that nation. A government issued letter of marque (and reprise) 'allowed merchants to attack any ship of the offending nation until they found something of equal value to their loss' [82, p. 231]. A number of the advisory reports take their inspiration from these 'letters of marque and reprisal'. Rabkin and Rabkin and Zarate want the US government to revive the practice for the cyber domain [78, pp. 2–3; 73]. However, Rosenzweig et al. note that though the analogy[5] has gotten quite some interest, letters of marque are not a good fit with the problems in cyber domain [77, pp. 7–8]. Two of their reasons have to do with the risk of escalation into international conflicts. First, they argue that letters of marque were effective because they motivate private actors through the profit motive and thus they could easily incentivize overly belligerent cyber aggression. In other words, they would neither be reliably under the control of the state—thus becoming a liability—nor would they be 'anchored' to the state in such a way that would bestow any political legitimacy. Here, private business interests could dramatically misalign with the public good. Cyber looting is likely to escalate conflicts. Secondly, the analogy fails to address the myriad of foreign domestic laws that are likely to be broken by such privateering. The internet may be global but, unlike the high seas, it is also to a large degree territorial and sovereign.

Whatever the exact form of licensing, the main risks involved will likely come from outside of the borders of the USA. Those are risks for the companies involved as well as for the United States as a sovereign state. Escalation of a hack into a conflict—especially when state actors are involved—is not an imaginary risk when non-state actors enter the scene of international security. Rosenzweig et al. therefore argue that any licensing should come with a framework that would ease 'the vigilante concern' that many in this field

5 For a more detailed analysis of privateering and the cyber domain, see [82].

have [77, p. 9]. That would still not solve the problem of American companies being in breach of foreign domestic law as these activities would be inherently transnational. Therefore, certification should not include authorization for hack back ('private cyber guards should have no authority to "return fire"') and should only empower companies to use tools in the "annoyance and attribution" parts of the gray zone. For the highest levels of ACD, i.e. hack backs, almost all reports are unanimous: only states have the legal right to execute these. However, many reports also advocate that at these levels private companies could have some sort of deputy sheriff's role. Close collaboration with law enforcement and the provision of forensic proof for attribution could help solve the government's problems with capability and capacity. To Rosenzweig et al. that should come with a quid pro quo: it requires the state to step up its activities of persecution and retaliation. 'While not every piece of intelligence can be acted on or used in court, it is not unreasonable to expect the government to be more vigorous in its investigation and prosecution of cybercrime' [77, p. 10]. This argument can also be seen as a roundabout way of putting pressure on the government to step up its game, addressing not so much the capacity problem, but the problem of political will. Although the reports are not very explicit as to how far private solutions should be allowed to venture into the dark grey zone, the field starts to diverge in how aggressive they would allow private ACD (in the abstract) to be.

External effects: liability and international security and diplomacy

A market for commercial active cyber defense means that—licensed—cyber security firms would be able to operate across the boundaries of third-party networks and/or across different international jurisdictions. Especially when working for high-end, internationally operating clients, the work of private cyber security firms would take place at the intersection of the domestic and the international. Two likely external effects to consider would be that their actions may do (i) damage to (innocent) third parties and (ii) may create political tensions with the countries in which they operate.

The proposed legal changes and certifications schemes mainly address, the *domestic* tension between the (prohibited) private use of force and internal state sovereignty. They mainly try to solve the problem of the underperformance of the state in the provision of cyber security without undercutting its sovereign rights. When taking in the overall gist of the reports, the answer in a nutshell is to use, and sometimes 'enlist', private capacity and anchor it to state legitimacy through certification schemes and (mandatory) cooperation with law enforcement when a higher level use of force is required. Moving the state in as the central anchoring node is seen as the key to legitimacy. However, as the problem of cyber security provision is situated at the intersection of internal and external sovereignty, more is needed. What happens if ACD escalates through counter actions from states, cyber criminals or from damages done to third-party networks that were not implicated in malicious behavior? The first line of defense is cooperation with state law enforcement in the higher spectrum of the use of force, as discussed above. If corporations are 'just the deputies' then it is the sheriff that provides the international legitimacy and takes responsibility in the realm of international relations. The second line is to shield companies from prosecution, either formally or informally. The third line is to engage internationally with other states to advance the idea and acceptability of ACD as a norm at the international level.

The easiest way to shield companies is to exempt them from prosecution. Many maintain that this is already happening informally, because even though it is assumed that ACD is happening, there is hardly any case law. The Center for Cyber and Homeland Security on the basis of their discussion of the Google Aurora case see evidence of an informal exemption of liability and advocates to elevate this practice to the level of principle: 'Companies engaging in activities that may push the limits of the law (. . .) should not be prioritized for investigation or prosecution' [9, p. 14]. Some argue for legal exemptions, for example Rosenzweig et al. advocate legal liability exceptions for certified companies in case of beaconing (which is at odds with CFAA) and also for some forensic intelligence work [77, p. 10]. This is quite similar to the provision in the draft ACDC bill that gives exemption of legal liability for those taking active cyber defense measures, 'meaning unauthorized access to the attackers computer to (a) establish attribution, (b) disrupt the attack ("disrupt continued unauthorized activity"), (c) monitor attackers behaviour to improve defense'. Rosenzweig et al. specifically address the problem of *foreign* legal charges by urging the government to:

> Explore legal options to protect businesses and individuals that engage in authorized active cyber defenses. As there are obstacles to active defense in foreign law, the U.S. government should assure cyber private responders that it will shield them from foreign criminal liability so long as they abide by the terms of their license and do not attack foreign systems [77, p. 11].

Lastly, and conversely, Hofmann and Levite who argue for a more loosely and privately organized regime for certification, present liability as a means to keep private ACD in check and argue that the defender 'should be liable for damage and/or the disruption of legitimate services it causes to innocent third parties', especially when behaving excessively or when abusing its mandate [76, p. 36]. Here liability would be used to address vigilante concerns. Most of this is predominantly focused on the domestic side of the argument though, the international side does not get much of a look in.

Internationally, legally sanctioning private active cyber defence puts the American government on the spot. If it would move forward on ACD, the USA it would be the first state to formally unleash its private sector and create a new cyber security actor that is legally sanctioned at the national level, which would not go unnoticed internationally. Some reports therefore also call for a diplomatic initiative. Hoffman and Levite argue: 'The pitfalls inherent in unilateral state solutions, even in powerful and influential states such as the United States, are simply untenable. Creative mechanisms to regulate this activity globally will be crucial for the creation of legitimate space for private sector ACD' [76, p. 5]. Zarate [73] and the Center for Cyber and Homeland Security [9, p. xiii] agree, while Hoffman and Levite warn that 'achieving consensus on a global treaty to regulate this space would require strenuous and time-consuming efforts, if it is attainable at all' [76, pp. 36-7]. Rosenzweig et al. propose a slightly more modest approach, starting with American allies:

> The U.S. should work with its allies to promote a system that authorizes U.S. and allied private cybersecurity providers to digitally follow malicious hackers across state lines under certain circumstances and rules. While there will inevitably be cases of friendly fire or collateral damage, the deterrent and punishing effect should be impressed upon U.S. allies in order to come to a cyber-self-defense agreement [77, p. 11].

However, the *Paris Call for Trust and Security in Cyberspace* [83], which is the only international document mentioning private active cyber defence and is signed by most of America's European

allies, explicitly takes position against private hack backs, making any international agreement—even among allies—more of an uphill battle. Should the US move the legal lines for private ACD it will ruffle international feathers but also create a new practice on the ground. If US companies are allowed a certain measure of self-defence at the international level with the political and legal backing of their own government, other countries may move in a similar direction. As Bruce Schneier noted in the context of the debate on backdoors: there is no such thing as a back door that only the good guys walk through' [84]. It would not be the first time that American unilateralism has paved the way for change.

Conclusion

Private sector Active Cyber Defence lies squarely on the intersection of domestic security and international security. Domestic legislation that would legally allow private active cyber defence would need to be reconciled with the state's domestic monopoly on the legitimate use of force and—given the inherent transnational nature of the internet—would have to address the issue of private companies potentially disrupting state-to-state relations, creating or exacerbating international tensions and more generally trespassing on what states consider their *domain reservé*. Generally, public–private governance solutions for security problems always have to find a way to manage a balance between (i) questions of capacity and assigning responsibilities, (ii) the political legitimacy of public-private security solutions, and (iii) the mitigation of their external effects. Private active cyber defence provides a difficult case to get this balancing act right. This article looked at the theory and practice of private cyber security provision and analysed in more detail a number of recent reports and publications by Washington DC based commissions and think tanks that propose legalizing forms of active cyber defence, in which private cyber security companies would be allowed to operate beyond their own, or their clients' networks, and push beyond American law as it currently stands.

The case of the public–private cyber security governance, and the more detailed analysis of American think tank proposals on active cyber defence, reveals a strong emphasis on addressing the domestic security (and political) problem: the aim is to solve the capacity problem by creating room for private cyber security solutions through new legislation and the regulation of a new security market. This market would be anchored to the state through legislation and certification schemes to make the solution politically legitimate. At the domestic level, one could say that this contributes both to the output legitimacy (increasing capacity) and input legitimacy (creating a legal basis and sharing in the legitimacy of the state as a security actor) of the scheme. The proposals balance capacity, new responsibilities and address the matter of domestic political legitimacy. The proposals also lack specificity: urging the government to move on expanding the possibilities for ACD, while reluctant to be very specific about which measures would be allowed under which circumstances. The major problem however lies with the international political legitimacy, especially in light of possible external effects at the international level. Although most reports acknowledge the tension between private ACD and the political dimension of international cyber security—including the risk of escalation of international tension and conflict—they lack realistic proposals to address these tensions. The reports anticipate international pushback, but offer little to mitigate it, while active cyber defence measures by private companies in the current geopolitical climate would most likely be received internationally as an escalatory and provocative policy. If the US government would certify private cyber security companies to engage in ACD they could be easily be marked as government proxies—albeit more in a political than a legal sense. Internationally, there does not seem to be much appetite among US allies to embark on a diplomatic road to legitimize and codify private cyber security companies to operate at the international level. If anything, the diplomatic deck is stacked against the idea, as evidenced by one of the norms in the *Paris Call for Trust and Security in Cyberspace*. Should the USA move forward on the idea of private active cyber defence it will likely be perceived as American exceptionalism, which will fail to convince allies of its merits, and may embolden upcoming powers like China who will claim the same rights of exceptionalism for themselves as they rise [48].

The practical and political risks at the international level and the fact that many of the reports—some written by former government officials—flag the issue but fail to address it in any substance, gives pause for thought. How serious are these reports in their desire to actually take decisive steps forward in the 'debate that does not go away'? How serious are their proposals to let private cyber security companies become international security actors? As the reports and policy suggestions are skewed towards the domestic debate, it is possible that their aim may be to influence the debate about the root problem of companies feeling unprotected in different ways than just the one that is explicitly addressed. One implicit message that can be read into some of these reports, would be that governments need to step up their game—or bear the risk of private solutions that may be hard to control and may undercut government legitimacy. Similarly, it could be a message to private companies to step up the protection of their digital assets and by extension the general cyber security of the private sector. Knowing that the more invasive parts of the ACD continuum are unlikely to find their way into law, think tankers and former government officials may see the debate about ACD as an opportunity to get in the low hanging fruit of the clarification of the law, and counter the problem of underinvestment in cyber security in the private sector.

Acknowledgements

The author would like to thank the participants of the 2019 The Hague Cyber Norms Conference and the two anonymous reviewers for their comments and suggestions. The author is most grateful to Madeline Carr for her insightful and constructive comments on an earlier version of this article and to Corianne Oosterbaan for copyediting this article.

Funding

The work of the author and the Hague Program for Cyber Norms is supported by a grant of the Dutch Ministry of Foreign Affairs.

References

1. World Economic Forum. *Regional Risks for Doing Business 2018*, Insight report. Geneva: World Economic Forum, 2018.[TQ1]
2. Carr M. Public-private partnerships in national cyber-security strategies. *Int Aff* 2016;**92**:43–62.
3. Dunn Cavelty M. From Cyber-bombs to political fallout: threat representations with an impact in the cyber-security discourse. *Int Stud Rev* 2013; **15**:105–22.
4. Dunn Cavelty M, Suter M. Public-private partnerships are no silver bullet: an expanded governance model for critical infrastructure protection. *Int J Crit Infrastruct Prot* 2009;**2**:179–187.
5. Arnold M, Brathwaite T, Kuchler H. Davos 2015: Banks call for free rein to fight cybercrime. *Financial Times* (22 January 2015).

6. Zarate J. The cyber financial wars on the horizon: the convergence of financial and cyber warfare and the need for a 21st century national security response. In: Ravich S (ed.), *Cyber Enabled Economic Warfare: An Evolving Challenge*. Washington, DC: Hudson Institute, 2015, 93–120.
7. Chesney R. *Hackback is Back: Assessing the Active Cyber Defense Certainty Act*. *Lawfare* (14 June 2019): https://www.lawfareblog.com/hackback-back-assessing-active-cyber-defense-certainty-act. (21 February 2021, date last accessed).
8. Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong (2017): https://www.congress.gov/115/bills/hr4036/BILLS-115hr4036ih.pdf. (21 February 2021, date last accessed).
9. Center for Cyber and Homeland Security. *Into the Gray Zone. The Private Sector and Active Defense against Cyber Threats*. Washington: George Washington University, 2016.
10. Abrahamsen R, Williams MM. Security beyond the state: global security assemblages in international politics. *Int Political Sociol* 2009;**3**:1–17.
11. Abrahamsen R, Williams MC. *Security Beyond the State: Private Security in International Politics*. Cambridge: Cambridge University Press, 2011.
12. Singer P. *Corporate Warriors: The Rise of Privatized Military Industry*. Ithaca: Cornell University Press, 2003.
13. Leander A. The power to construct international security: on the significance of private military companies. *Millenn J Int Stud* 2005;**33**:803–826.
14. Gould A. Global assemblages and counter-piracy: public and private maritime policing. *Polic Soc* 2017;**27**:408–418.
15. Broeders D. The hybridization of cyber security governance: the emergence of global cyber security assemblages. *Glob Policy Digit Debates* 2017;Special Issue: 38–44.
16. Collier J. Cyber security assemblages: a framework for understanding the dynamic and contested nature of security provision. *Politics Gov* 2018;**6**: 13–21.
17. Broeders D. *The Public Core of the Internet: An International Agenda for Internet Governance*. Amsterdam: Amsterdam University Press, 2015.
18. Deibert R. *Black Code. Inside the Battle for Cyber Space*. Toronto: Signal, 2013.
19. DeNardis L. *The Global War for Internet Governance*. New Haven and London: Yale University Press, 2014.
20. Lachow I, Grossman T. Cyberwar Inc.: examining the role of companies in offensive cyber operations. In: Lin H, Zegart A (eds), *Bytes, Bombs and Spies. The Strategic Dimensions of Offensive Cyber Operations*. Washington DC: Brookings Institution Press, 2018, 379–99.
21. Maurer T. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge: Cambridge University Press, 2018.
22. Harris S. *@War: The Rise of the Military Industry Complex*. Boston and New York: Houghton Mifflin Harcourt, 2014.
23. Boeke S, Heinl C, Veenendaal M. Civil-military relations and international military cooperation in cyber security: Common challenges & state practices across Asia and Europe. *Cyber Conflict: Architectures in Cyberspace (CyCon), IEEE Seventh Int Conf on Cyber Conflict: Architectures in Cyberspace (CyCon)*, 2015: 69–80.
24. Bossong R, Wagner B. A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime Law Soc Change* 2017;**67**: 265–88.
25. Boeke S. National cyber crisis management: different European approaches. *Governance* 2018;**31**:449–64.
26. Weiss M, Jankauskas V. Securing cyberspace: how states design governance arrangements. *Governance* 2019;**32**:259–75.
27. Shearing C, Wood J. Nodal governance, democracy, and the new 'denizens'. *J Law Soc* 2003;**30**:400–19.
28. Loader I, Walker N. *Civilizing Security*. Cambridge: Cambridge University Press, 2007.
29. White A. The new political economy of private security. *Theor Criminol* 2012;**16**:85–101.
30. Scarpello F. Toward the political economy of plural policing: tacking stock of a burgeoning literature. *Int Stud Rev* 2017;**19**:407–29.
31. Chang LYC, Zhong LY, Grabosky PN. Citizen co-production of cyber security: self-help, vigilantes and cybercrime. *Regul Gov* 2018;**12**:101–14.
32. Valeriano B, Maness RC. *Cyber War versus Cyber Realities. Cyber Conflict in the International System*. Oxford: Oxford University Press, 2015.
33. Garland D. *Culture of Control: Crime and Social Order in Contemporary Society*. Chicago: University of Chicago Press, 2001.
34. Dupont B. Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime Law Soc Change* 2017;**67**:97–116.
35. White A. *The Politics of Private Security*. Basingstoke: Palgrave Macmillan, 2010.
36. Scharpf F. *Governing Europe: Effective and Democratic?* Oxford: Oxford University Press, 1999.
37. Börzel T, Risse T. Governance without a state. Can it work? *Regul Gov* 2010;**4**:113–34.
38. Börzel T, Tisse T. Public-private partnerships: effective and legitimate tools of transnational governance? In: Grande E, Pauly L (eds), *Complex Sovereignty: Reconstituting Political Authority in the 21st Century*. Toronto: University of Toronto Press, 2005, 195–216.
39. Schäferhoff M, Campe S, Kaan C. Transnational public-private partnerships in international relations: making sense of concepts, research frameworks, and results. *Int Stud Rev* 2009;**11**:451–74.
40. Weber M. *The Vocation Lectures. Science as a Vocation/Politics as a Vocation*. Cambridge (Indianapolis): Hackett Publishing, 2004/1919.
41. Thompson JE. *Mercenaries, Pirates & Sovereigns*. Princeton: Princeton University Press, 1994.
42. Kello L. *The Virtual Weapon and International Order*. New Haven: Yale University Press, 2017, 190–92.
43. De Carvalho B, Leira H, Hobson J. The big bangs of IR: the myths that your teachers still tell you about 1648 and 1919. *Millennium* 2011;**39**: 735–58.
44. Demchak C, Dombrowski P. Cyber Westphalia: asserting state prerogatives in cyberspace. *Georget J Int Aff* 2013;Special Issue: 29–38.
45. Lewis J. *Internet Governance: Inevitable Transitions*. CIGI Internet Governance Papers no. 4 (October 2013).
46. Creemers R. China's conception of cyber sovereignty: rhetoric and realization. In: Broeders D, van den Berg B (eds), *Governing cyberspace: behavior, power, and diplomacy*. London: Rowman and Littlefield, 2020, 107–44.
47. Kurowska X. What does Russia want in cyber diplomacy? A primer. In: Broeders D, van den Berg B (eds), *Governing Cyberspace: Behavior, Power, and Diplomacy*. London: Rowman and Littlefield, 2020, 85–106.
48. Broeders D, Adamson L, Creemers R. *Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace*. The Hague: The Hague Program for Cyber Norms Policy Brief, 2019.
49. Segal A. When China rules the web: technology in service of the state. *Foreign Aff* 2018;**97**:10–18.
50. Krasner S. *Sovereignty: Organized Hypocrisy*. Princeton, NJ: Princeton University Press, 1999.
51. Mueller M. Against sovereignty in cyberspace. *Int Stud Rev* 2020; 22: 779–801.
52. Schmitt MN (ed.). *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. New York: Cambridge University Press, 2017.
53. Broeders D, Taylor L. Does great power come with great responsibility? The need to talk about corporate political responsibility. In: Taddeo M, Floridi L. (eds), *The Responsibilities of Online Service Providers*. New York: Springer, 2017, 315–23.
54. Broeders D, De Busser E, Pawlak P. *Three Tales of Attribution in Cyberspace: Criminal Law, International Law and Policy Debates*. The Hague: The Hague Program for Cyber Norms Policy Brief, 2020.
55. Egloff F. Contested public attributions of cyber incidents and the role of academia. *Contemp Secur Policy* 2020;**41**:55–81.
56. Roguski P. *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*. The Hague: The Hague Program for Cyber Norms Policy Brief, 2020.
57. Maurer T. 'Proxies' and Cyberspace. *J Confl Sec Law* 2016;**21**:383–403.
58. Buchanan B. *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. Oxford: Oxford University Press, 2016.

59. Fisher M. *Should the U.S. Allow Companies to 'Hack Back' Against Foreign Cyber Spies?*. The Washington Post (23 May 2013).
60. Ponta A. Cyber Operations Against Medical Facilities During Peacetime. *Lawfare* (1 May 2020): https://www.lawfareblog.com/cyber-operations-against-medical-facilities-during-peacetime. (21 February 2021, date last accessed).
61. Cook C. Cross-border data access and active cyber defense: assessing legislative options for a new international cyber security rulebook. *Stanf Law Policy Rev* 2018;**29**:205–36.
62. Nusca A. Hayden: 'Digital Blackwater' may be necessary for private sector to fight cyber threats. *ZD Net* (1 August 2011): https://www.zdnet.com/article/hayden-digital-blackwater-may-be-necessary-for-private-sector-to-fight-cyber-threats/. (21 February 2021, date last accessed).
63. Maschmeyer L, Deibert RJ, Lindsay JR. A tale of two cybers – how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *J Inf Technol Politics* 2021;**18**:1–20. 10.1080/19331681.2020.1776658.
64. Healey J, Jenkins N, Work JD. Defenders disrupting adversaries: framework, dataset, and case studies of disruptive counter-cyber operations. In: Jancárková T, Lindström L, Signoretti M, Tolga I, Visky G (eds), *20/20 Vision. The Next Decade*. 12th International Conference on Cyber Conflict, IEEE, 2020, 251–74.
65. van Eeten MJG, Bauer JM, Asghari H, *et al. The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data*. Paris: OECD, 2010.
66. Asghari H, van Eeten MJG, Bauer JM. Economics of fighting botnets: lessons from a decade of mitigation. *IEEE Secur Priv* 2015;**13**:16–23.
67. Tan J, Tan AE. Business under threat, technology under attack, ethics under fire: the experience of google in China. *J Bus Ethics* 2012;**110**:469–79.
68. Timberg C, Nakashima E, Douglas-Gabriel D. Cyberattacks trigger talk of 'hacking back'. *The Washington Post* (9 October 2014).
69. Sobczak B. Grid hackers can expect retaliation, CEO warns. *E&E News* (27 June 2018): https://www.eenews.net/stories/1060086575/print. (21 February 2021, date last accessed).
70. Weidenbaum M. *The Competition of Ideas: The World of the Washington Think Tanks*. New Brunswick, NJ: Transaction Publishers, 2008.
71. Foundation for Defense of Democracies, *Wikipedia*: https://en.wikipedia.org/wiki/Foundation_for_Defense_of_Democracies (28 November 2020, date last accessed).
72. Lachow I. *Active Cyber Defense, a Framework for Policy Makers*. Policy brief, Washington DC: Center for a New American Security, 2013.
73. Zarate J. *The Cyber Financial Wars on the Horizon: The Convergence of Financial and Cyber Warfare and the Need for a 21st Century National Security Response*. Washington DC: Foundation for Defense of Democracies, 2015.
74. Commission on the Theft of American Intellectual Property. The IP Commission Report. Washington DC: The IP Commission, 2013.
75. Nelson S. 'Active cyber defense' or vigilantism? *Washington Examiner* (13 February 2018): https://www.washingtonexaminer.com/active-cyber-defense-or-vigilantism. (21 February 2021, date last accessed).
76. Hoffman W, Levite AE. *Private Sector Cyber Defense, Can Active Measures Help Stabilize Cyberspace?* Washington DC: The Carnegie Endowment for International Peace, 2017.
77. Rosenzweig P, Bucci SP, Inserra D. *Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense*, Backgrounder no. 3188, The Heritage Foundation (5 May 2017).
78. Rabkin A, Rabkin J. *Enhancing Network Security. A Cyber Strategy for the Next Administration*. AEI Technology Policy Working Paper 2016-01, Washington DC: American Enterprise Institute (May 2016).
79. Rosenzweig P. International Law and Private Actor Cyber Defensive Measures. *Stanf J Int Law* 2013;**50**:103–118.
80. Sanger D. *The Perfect Weapon. War, Sabotage, and Fear in the Cyber Age*. London: Scribe Publications, 2018.
81. Fire-Eye. Doing Our Part – Without Hacking Back. *Executive Perspectives* (25 June 2018): https://www.fireeye.com/blog/executive-perspective/2018/06/doing-our-part-without-hacking-back.html. (21 February 2021, date last accessed).
82. Egloff F. Cybersecurity and the age of privateering. In: Perkovitch G, Levite AE (eds), *Understanding Cyber Conflict: Fourteen Analogies*. Washington DC: Georgetown University Press, 2017, 231–47.
83. France D. Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace, 2018: https://www.diplomatie.gouv.fr/en/french-foreign-policy/united-nations/alliance-for-multilateralism-63158/article/paris-call-for-trust-and-security-in-cyberspace. (21 February 2021, date last accessed).
84. Schneier B. iPhone Encryption and the Return of the Crypto Wars. *Schneier on Security* (6 October 2014): https://www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html. (21 February 2021, date last accessed).