Chapter 16
A Framework for Ethical Cyber-Defence for Companies

Salome Stevens

Abstract Private sector companies are becoming increasingly frustrated over the lack of effective solutions to growing criminal threats in cyberspace, leading to calls by security experts for a more active cyber-defence including offensive actions in cyberspace taken with defensive purposes in mind. However, should private companies use active cyber-defence measures or would they by such an act implicate themselves in illegal actions? As long as there is no specific regulation defining the legal grounds for active cyber-defence, the conventional doctrine of a right to self-defence may be the closest analogy within the physical realm. This chapter examines cyber-defence along the lines of a right to self-defence and concludes that the categorisation of passive and active does not allow for a thorough analysis of the legal and ethical justification of a specific defensive measure. Instead, a categorisation based on the effects of a specific measure is suggested. Along the lines of this effect-based categorisation—and considering the capabilities as well as the limits of the application of a right to self-defence to cyberspace—this chapter proposes some concrete recommendations for companies on how to define ethical cyber-defence within their security strategy.

Keywords Attribution · Necessity · Proportionality · Self-defence · Subsidiarity

16.1 Introduction

The number of cyberattacks have grown exponentially in recent years. As a consequence, private companies have invested more resources into building a cybersecurity strategy that uses digital tools to protect computer systems and networks from malicious intrusions. One way of doing this is the use of more active cyber-defence strategies (see for example Schmidle 2018). However, how far can a company go before it crosses the line and implicates itself into committing illegal actions? In the

S. Stevens (✉)
Institute of Criminal Law, Criminal Procedural Law and International Criminal Law, University of Zurich, Zurich, Switzerland

M. Christen et al. (eds.), *The Ethics of Cybersecurity*, The International Library of Ethics, Law and Technology 21,
https://doi.org/10.1007/978-3-030-29053-5_16

absence of any legal regulation on the use of cyber-defence for private companies, this chapter examines cyber-defence along the lines of a right to self-defence within the physical realm. It begins with a straightforward question underlying this article: Should a company use active cyber-defence? It then examines cyber-defence from the perspective of a right to self-defence, which considers not only the final effects of a cyber-defence measure, but also the circumstances in which the measure is applied. The chapter concludes with some concrete recommendations for companies regarding what to consider when defining ethical cyber-defence within their security strategy.

16.2 Should a Company Use Active Cyber-Defence?

Whereas there have been a number of different attempts to classify cyber-defence, the distinction between 'active cyber-defence' and 'passive cyber-defence' is the most common one. There are differing definitions of what active and passive could mean in the context of cyber-defence. Denning and Strawser define active cyber-defence as any "direct defensive action taken to destroy, nullify, or reduce the effectiveness of cyber threats (…)" and passive cyber defence as "all measures, other than active cyber defence, taken to minimise the effectiveness of cyber threats" (Denning and Strawser 2017: 3). However, if we examine cyber-defence from a right to self-defence, then the distinction between active– and passive defence becomes less relevant, as they can in principle both be legitimised under the right to self-defence and there are few cases where one would be obliged to revert to passive– defensive measures. For the above reason, we choose to add another description to the usual categorisation of passive and active defence; one which considers the effects of a specific measure rather than its characteristics. Therefore, a specific cyber-defence measure could either have the effect of breaking the law or not.

Returning to the categorisation of active and passive cyber-defence, some defensive measures showing an active component are clearly against the law. Gaining unauthorised access to a computer system for example, or 'hacking' is illegal in most countries (on hacking see Chap. 8). Consequently, this is the case also for 'hacking back'. As a result, a company deciding to infiltrate another computer system or network without the permission of the user or network owner is breaking the law in the same way the initial attacker does. The same could be said for such active defensive measures that destruct external networks or data. For this reason, we here categorise such cyber-defence measures that regularly break the law as being problematic cyber-defence measures.

Passive cyber-defence measures on the other hand, such as a firewall, an antivirus or an encryption program, would regularly not break any law, because they would not create any negative effects. We call these measures unproblematic.

However, more interestingly, some cyber-defence measures with an active component could either be problematic or unproblematic depending on the manner in which they are used. Such defensive measures would fall within a grey zone, being

Table 16.1 Application of a second layer of categorisation to cyber-defence

Definition based on the **characteristics** of the cyber-defence measure	**Passive cyber-defence**	**Active cyber-defence**	
Definition based on the **effects** of the cyber-defence measure	**Unproblematic cyber-defence measures** For example Firewalls, antivirus, encryption programs	**Grey zone** For example IT blocking, traffic deflecting, honeypots, beacons	**Problematic cyber-defence measures** For example hacking back, disruption or destruction of external networks or data

neither clearly problematic nor unproblematic. An Internet Protocol (IP) blocking, traffic deflection or a honeypot, for example, could be within the law if it does not inflict any harm on third parties. The same could possibly count for beacons or white-hat ransomware depending on the manner in which they are being applied (Hoffman and Nyikos 2018: 17–25, 51; for a conceptualisation of different defence measures see Chap. 2).

Consequently, our categorisation results in the distinction of three different groups: Defensive measures that are regularly unproblematic (marked in white in Table 16.1), defensive measures that may be problematic depending on their concrete application (marked in light grey in Table 16.1) and defensive measures that regularly fall within the category of problematic defensive measures (marked in dark grey in Table 16.1).

From this new effect-based categorisation of cyber-defence measures, we conclude that the question of whether a company may use active defence in its security strategy is formulated too broadly, and the fact that a defensive measure shows an active component does not directly imply its unlawfulness. Even if some active cyber-defence measures could imply a higher risk for companies (problematic measures marked in red in Table 8), the question of whether a specific active defence measure could break the law should be analysed on a case-by case-basis and demand the careful consideration of the potential effects it may cause in the given circumstances vis-à-vis the laws that may apply to a given situation. Such evaluation requires the consideration of direct as well as secondary or unintended effects that result from the application of a specific measure.

16.3 Applying Self-Defence to Cyber-Defence

The right to self-defence as considered in this chapter is incorporated in criminal law and aims to regulate the conduct of private citizens. As such it is to be distinguished from the concept of self-defence in international public law, which regulates the right of states to apply force in response to armed attacks. Self-defence—as defined

in criminal law—can allow for the use of force against an attacker and thus render an otherwise illegal act lawful, provided it was necessary to defend one's own interests. Self-defence is recognised by a majority if not all domestic legal systems and has found recognition as a legal principle in core disciplines of international law (on self-defence in international law see: Hessbruegge 2017). Common law jurisdictions distinguish between defence of oneself, defence of others, and defence of property, while most civil law systems include all three concepts under the notion of legitimate self-defence (Hessbruegge 2017: 4). Although this chapter attempts to provide a holistic understanding on the ethical implications of cyber-defence, some of the following considerations may be based on the notion of self-defence under the Swiss Criminal Code (SCC) (see Art. 15–18 SCC).

If we are to apply the principle of self-defence to the categorisation of cyber-defence measures into problematic and unproblematic measures (cf. Sect. 16.4), then the parameters could shift once again. Whereas the categorisation in Sect. 16.3 emphasises the final effect—the result—of an applied defensive measure, the paradigm of self-defence considers the circumstances that led to the application of the said measure. As a result, even such active cyber-defence measures that fall within the category of problematic cyber-defence measures could in principle be justified under law and thus rendered lawful, provided they fulfil the requirements of an act of self-defence. To illustrate, consider a person using force against a thief to safeguard his or her property. Most people would approve of the defender's act even if in principle it breaks the law. This is, of course, depending on how much force the defender applies. Whether the same could apply for a company's security team using force on an attacker's computer system or network to ward off a cyberattack is to be explored in the following sections.

16.4 Could Self-Defence Justify Cyber-Defence Otherwise Considered Unlawful?

Unsuprisingly, self-defence provisions were drafted for a physical realm, far before a scenario of active cyber-defence was foreseen, and up until today there has been no relevant case law on the application of self-defence to the realm of the cyber world. This is why it remains uncertain if and how the right to self-defence would apply to cyber-defence by a private company. It could be argued that the physical paradigm of self-defence is unsuited to draw the line between such cyber-defence measures that may be deemed acceptable under law and ones that should be forbidden by it. The argument fundamentally rests on the assumption that active cyber-defence is essentially different from any conventional case of self-defence, which is why the conventional self-defence doctrine cannot tackle the particularities of cyber-defence. We examine some of the most prominent claims against applying self-defence to cyberspace.

16.4.1 The Argument of Vigilantism

It has been argued that the particularities of active cyber-defence measures are such that they are never defensive but rather serve revenge goals or deter future attacks. This is why a majority of cybersecurity experts say that the right solution in response to a cyberattack is always be to leave the matter in the hands of law enforcement (see, for example, reader comments to Volokh 2007).

Self-defence is indeed to be distinguished from punishment. Whereas self-defence can only cover acts taken to prevent a harm, counteracting an attack may entail punishment. Actions of a punishing nature, except for a few exceptions regarding minor criminal offences, are generally not allowed by contemporary domestic criminal orders. This is so because they go against the state's monopoly of the use of force. As a result, acts that are in breach of the state's monopoly of the use of force are generally considered acts of vigilantism (see also Dittrich and Himma 2005: 673 ff.).

In the realm of cyber-defence, this would mean that a legitimate act of defence must be able to stop an imminent unjust attack. If an applied technique of active cyber-defence cannot stop an imminent unjust attack, then it cannot be defensive but may, rather, be considered offensive (see also Denning and Strawser 2017: 11). The problem lies when such counteract is executed in a second moment, meaning when it is too late for it to be considered self-defence (see for example Fletcher 1989: 201). To illustrate, let us consider active cyber-defence techniques used for attribution, namely the identification of the perpetrators of the hacking attack. In a number of cases, such techniques may be applied after an attack has occurred and may be used to report an attacker to the authorities or to send a strong message of deterrent to the attackers. Accordingly, such active cyber-defence techniques applied for the purpose of attributing the initial attack to the perpetrators may be said to have a primarily punishing or retaliatory nature rather than a defensive one (see also Himma 2004: 4). Thus, they would be unjustified under self-defence. This may, however, not be the case if the cyberattack is to be considered ongoing (on this point see Sect. 16.4.2) and if the attribution measure is applied with the aim of ending the attack. Furthermore, if we consider the blockage of traffic coming from a malicious IP address, then this active measure could in principle be defensive in nature.

Based on the above considerations, it would be premature to conclude that every measure of active cyber-defence would necessarily always have to be vigilant. In the end, it is precisely the aim of any self-defence provision to be outlined in such a way as to reliably draw the line between defensive and retaliatory measures. To define the defensive element of an act, it has to incorporate several indicative elements. An act can thus only be considered a case of self-defence if it satisfies the requirements of self-defence, namely if (1) It comes as a direct response to an imminent unlawful attack (2) It is necessary to ward off the attack, and (3) The preserved interest is not disproportionate to the harm inflicted on the attacker (based on Art. 15 SCC as commented in Niggli and Göhlich 2019a, b with further references).

16.4.2 The Argument of the Speed of Cyberattacks

If we take the example of the requirement of imminence of an attack, then we come across several situations where the term demands further clarification within a scenario of active cyber-defence. One peculiarity of cyberattacks is their speed, which often outpaces human-dependent cyber-defence. In the case of encryption, for example, most ransomware can complete encryption within less than 1 min after intrusion. In the case of cyber-defence, this would mean that any justifiable active defence measure would have to happen within these couple of seconds before successful encryption. It is unlikely that any human-dependent cyber-defence system could act timely in this case even if intrusion is detected before encryption is completed. The technical characteristics of the speed of such cyberattacks would thus render the proof of imminence of any cyber-defensive action close to impossible.

A similar line of argument could apply to preventive defensive measures, namely such measures that are applied in advance of an attack and aim to prevent an attack from happening. While the requirement of imminence does not oblige a defender to wait with the defensive action until it is too late to effectively defend oneself, the lawful application of a preventive defensive measure in cyberspace would essentially require a company to have known about the attack in its planning phase. Considering the limitations of the legal possibilities of private companies to gather intelligence outside of their own network, it is unlikely that a company would be aware of a planned attack on itself to such a degree that a preventive counterstrike could comply with the requirement of imminence for a situation of self-defence (Stevens 2019: 326 ff. with further references).

Consequently, the requirement of imminence significantly narrows the scope of situations of cyberattacks in which self-defence could apply. Essentially, self-defence in cyberspace would be limited to cyberattacks that imply the resilience of a cyber-attacker within a company's system or network for a prolonged period of time or to such attacks that entail some sort of persistent attacking behaviour, as for example in the case of a Distributed Denial of Service (DDoS) attack or possibly even the intrusion sequences of a cyber kill chain (for a consideration of this argument see Stevens 2019: 335 ff.; on the conceptualisation of a cyber kill chain see Chap. 2).

16.4.3 The Argument of the Harm to Innocent Third Parties

Because the right to self-defence relies essentially on the distinction between an attacker and innocent third parties, attribution is a central element of every case of self-defence. It answers the question of who is to be held responsible for an attack and consequently against whom a defensive measure may be justified. The nature of cyberspace, however, makes it particularly easy for attackers to hide their identity through third-party systems, which get hijacked for the purpose of initiating an attack. This is why in the realm of cyber-defence, an attack needs to be attributed on several levels: (1) It needs to be attributed to a specific computer or server; (2) The identified computer or server needs to be attributed to an owner or legitimate user(s);

and (3) The attack needs to be attributed to the specific person or organisation that is behind it.

The challenges connected to the attribution of cyberattacks thus puts active cyber-defence at particular risk of causing unintended damage to innocent third-party computer- or server users. In extreme situations, an active countermeasure against the source of a cyberattack could lead to the disruption or destruction of a hospital's computer system, thereby indirectly causing physical harm or even death to patients who rely on the functioning of the hijacked computer system. Considering the risks of false attribution in cyberspace, it is argued that the best way to avoid the uncertainties related to the attribution of cyberattacks would be to completely forbid any problematic defence measure in cyberspace.

Generally speaking, self-defence does not justify harm inflicted on an innocent third-party. Its parameters are limited to acts directed against the person to which the attack can be attributed. However, in some particular circumstances, criminal behaviour against an innocent third-party may still be justified defence, for example: (1) If the defender had no other way to ward of the attack and the preserved interest weights proportionally more than the harm caused to innocent third-parties (i.e. situation of necessity); (2) If the defender reasonably believed that the act was directed against the attacker and would not inflict harm on any innocent third-party (i.e. error of fact; putative self-defence).

Whereas situation 1 essentially relies on the parameters of subsidiarity and proportionality of the applied defensive measure (cf. Sect. 16.4.4), situation 2 acknowledges the uncertainty of a given situation and allows for a reasonable margin of error (cf. Sect. 16.4.5). The question would thus be whether the defensive act against a third party could fulfil the requirements of subsidiarity and proportionality or whether it was the result of a reasonable error of fact in a given situation; both points discussed hereafter. It remains to be said that even if a right to self-defence could exclude criminal liability for a defensive act applied against a third party, the company could still face financial liability for the damage caused to the third party under tort laws. (based on Art. 52 II Swiss Code of Obligations (SCO)).

16.4.4 Subsidiarity and Proportionality

For an act to be considered defensive, it needs to be appropriate in view of the prevailing circumstances. The appropriateness of an act is measured using the notions of subsidiarity and proportionality (based on Art. 15 SCC as commented in Niggli and Göhlich 2019a, b, n 28 ff. with further references). It cannot be said with certainty how a court would apply the requirements of subsidiarity and proportionality to a case of cyber-defence as there is no relevant case law on this matter. However, subsidiarity would likely imply that the threat could not have been effectively averted or minimised using a less invasive measure or that the used measure could have been applied in a less invasive manner. Acts directed against third party-users would set stricter parameters to the requirement of subsidiarity; obliging a defender to revert to non-invasive defensive measures should they be appropriate to avoid the threat

(based on Art. 17 SCC as commented in Niggli and Göhlich 2019a, b: n 16 with further references). In practice this could mean that if a court finds that an attack could have effectively been stopped without inflicting damage on the third party, then it would not justify the use of any more invasive cyber-defence measure.

The requirement of proportionality would require a balance to be carefully struck between the imminent harm avoided by a company against the damage done to an innocent third party, and possibly also the initial attacker. The infliction of physical harm to hospital patients that are kept on life support by the hospital computer system would, for example, be disproportionate to the financial interest of a company and could thus not be justified under self-defence. It would be more difficult to strike a balance between the financial interest of a company and the financial interest of a cyber attacker or a third party computer user. Here again it can be noted that the requirements to proportionality would be higher if the act was to cause damage to a third party rather than the attacker. It is therefore to be expected that the safeguard of a financial interest of a company is unlikely to justify the considerable financial damage on a third-party user. This situation may be altered if the attack on the company could directly or indirectly result in physical harm. As has been shown, striking a balance between two interests is by no means an easy task; in practice it can prove quite challenging and because the equation of proportionality needs to consider all the prevailing circumstances, no general line can be drawn.

16.4.5 The Argument of Uncertainty

Recognising that the paradigm of self-defence depends essentially on the parameters of subsidiarity and proportionality, another aspect of attribution that should be discussed when considering the application of self-defence in cyberspace is uncertainty. To calculate the parameters of a certain defensive action, foreseeing the consequences of our actions is an inevitable necessity, as well as foreseeing the harm averted at least to a degree of reasonable certainty. Even if in very specific circumstances self-defence could justify the act of a defender who mistakenly believes the requirements of self-defence to be satisfied—even if objectively these requirements are not met (i.e. error of facts; putative self-defence; cf. Sect. 16.4.3)—such a right can only apply to the one whom truly errs. A defender knowingly accepting the uncertainty over all relevant factors of a defensive act no longer errs and can thus no longer benefit from a right to err (confirmed by the Swiss federal court in BGE 135 IV 12, E. 2.3.1).

This could mean that if a defender cannot reliably attribute the source of the attack to a person or a server to a specific user, then consequently he or she cannot calculate the effects of an active cyber-defence action nor in some cases the harm it aims to avert. Consequently, because the defender cannot calculate the effects of his or her act, he or she lacks reason to think that the requirements of self-defence could be satisfied (see also Dittrich and Himma: 675). This is especially true given that

many active cyber-defence tools operate automatically and do not give the opportunity to contextualise the circumstances of a particular situation (see also Denning and Strawser 2017: 12). To illustrate this, consider the case of data theft. Whereas the security team of a company could detect that someone had been in their system and had possibly stolen some internal data, it is likely that at the time at which they decide to get unauthorised access to the attacker's computer system, they would not know who the hackers were nor what they intended to do with the removed company information. If the security team does not know what harm the company or any third parties would face or whether the information has already been passed on at the moment of the hack, then how could they decide whether their counter-action is necessary or proportionate at that given moment?

Even if we argue that attribution can be done quite reliably on all levels if done by the right people with the relevant capabilities, the problematic factor of applying self-defence to cyber-defence lies in the fact that the reasonable certainty of attribution increases the more time is spent on such activities (see for example Lin 2016: 13; Rid and Buchanan 2015: 32). In fact, a reliable attribution of an attack asks for follow-up investigations that go beyond the initial attribution at the time of the detection of the intrusion (Lin 2016: 13). In the case of APT10 (Mandiant's naming of the Chinese Advanced Persistent Threats (APTs) group) for example, it took a group of anonymous researchers almost 2 years of investigation to identify what they thought was a hacking campaign masterminded by the Chinese government (Anonymous 2018). Considering the requirement of imminence of an attack discussed in Sect. 16.4.2, it becomes questionable if any attribution made to a degree of reasonable certainty could be concluded within the given time frame to make it possible for the defender to comply with the requirement of imminence (cf. Sect. 16.4.2). Furthermore, reliable attribution may require active cyber-defence techniques that would be considered within the realm of problematic defence measures and could thus be breaking the law. This would lead to the paradoxical situation of attribution being simultaneously the motive as well as the precondition of a justifiable defensive countermeasure. From the above, we conclude that the particular uncertainty connected to attacks in cyberspace could be the most convincing argument against the use of active cyber-defence in cyberspace.

16.4.6 Is Active Cyber-Defence Worth the Risk?

In addition to considering the legal legitimation of any active cyber-defence measure, it makes sense to weigh up the potential gains from deploying a problematic cyber-defence measure against the potential risks and drawbacks of that measure (see also Dewar 2017: 16). If a cyberattack cannot reliably be attributed, then a company can consequently not know who is behind the attack. It could, for example, be a skilled teenage hacker, operating from his or her living room, a bunch of criminals seeking financial gains, an organised crime group, a competing company

trying to gain insight into company operations and trade secrets, a group of activists hacking a private company for political or ideological reasons or an adversary country controlling strategic cyberattacks for political and economic reasons. In fact, even if a person operating a specific attack was identified, it is not certain that this person is also the mastermind behind the specific operation. Depending on who is on the other end, the tools at a cybersecurity team's hands may be very limited and counterattacks could provoke further and more harmful attacks on the company's system or even have the potential of escalating into hostilities between nations, with severe consequences.

16.4.7 The Cross-Border Element of Cyber-Defence

There are a number of scholars who support the claim that it is best to specifically regulate active cyber-defence in separate new legislation (see for example Brunoni 2016: 3). The need to further regulate active cyber-defence by private companies has been especially vocal among United States scholars (see for example Rabkin and Rabkin 2016) and on 25 May 2017, U.S. Congress Member Thomas Graves introduced the 'Active Cyber Defence Certainty Act'. The bill would amend the Computer Fraud and Abuse Act (CFAA), the U.S. legislation that made it a federal crime to access a protected computer without proper authorisation, so as to authorise certain active cyber-defence measures by private sector organisations that go beyond their own network. The bill currently in congress has been heavily disputed by cybersecurity experts, who fear allowing private companies to use active cyber-defence could create a 'cyber wild west' and make vigilantism the norm (Swinhoe 2018). Despite the potential consequences of changing the CFAA, the act has one important limitation: The bill does not specifically tackle nor prohibit cross-border active countermeasures, and this is where the situation becomes more challenging.

In fact, examining the highly interconnected cyber-space, it could be argued that by allowing companies to use active cyber-defence techniques at home it is likely to result in such companies stepping across their home jurisdiction boundaries and perpetrating attacks in other countries. In such an event, the affected country, for example France, whose policy stance prohibits private companies from using any active cyber-defence, will find the ones in charge of the execution of the measure as criminals under French law, regardless of how they may be considered under any other domestic law (Smolanoff and Brill 2018: 6 ff.). From there it is easy to imagine how what would at first may seem like a legitimate defensive act by a private company could lead to a conflictual claim of states over criminal jurisdiction of the respective cyber-defence act. In fact, the international nature of data flows may be the biggest obstacle to any attempt to regulate active cyber-defence for private companies on a national level.

16.5 Recommendations

Recalling the categorisation of defensive measures in Chap. 4, we conclude that, although in principle it cannot entirely be excluded that very specific cases of cyber-defence could fall under a right to self-defence, the nature of cyber-defence, such as the implied uncertainty connected to the attribution of cyber attacks (cf. Sect. 16.4.5ff.) and the likelihood of third party damages (cf. Sect. 16.4.3), pose significant challenges to the reinterpretation of a physical concept of self-defense to the cyber world and thus make the use of problematic cyber-defence measures (marked in red in Table 8) particularly risky for a private company. It is best to entirely avoid their use. This counts in particular for such defensive measures that could result in physical harm to innocent third parties (such as in the case of the unintended take-down of a hospital server or a critical infrastructure for example) or considerable financial damage, no matter how small the risk of such an outcome may be (see also: Hoffman and Nyikos 2018: 53). A private company considering the application of a problematic cyber-defence measure should also keep in mind that such an act may result in financial liability for damages caused to third parties.

The decision to revert from using a problematic defensive measure does not always come lightly (see also Chap. 2), especially when it means accepting considerable damage to the company and allowing the criminal to get away with his or her malicious attack. To avoid facing such a conflictual decision of whether to use a problematic cyber-defence measure, there are a number of security measures a company can take that typically fall within the category of unproblematic measures and that aim to prevent the negative effects of a cyberattack. Encryption could be such a preventive measure. This ensures that the company's data is encrypted in such a way that it makes it more difficult for an attacker to read data and consequently use it in a malicious manner against the company. Other examples of preventive measures could be to run a firewall or other suitable security programs. There are several other security tools and techniques that can ensure the continued functionality of a system and limit the damaging effects in case of a hacker attack (see Dewar 2017). Securing a data backup could, for example, be an effective measure to avoid losing access to company data as a consequence to a hacking attack. At the same time, a power station could ensure the continued supply of electricity in the case of an attack (Dewar 2017: 12; for a conceptualisation of different cyber-defence measures see also Chap. 2).

If applied consciously, a range of active cyber-defence measures placed in the grey zone of Table 8 could be useful to complete a security strategy, provided they are applied in such a way as to avoid any negative effects or create tension with other countries. Their application would demand a careful consideration of all related effects (direct and secondary) and should include not only the location of the effects (within own network or outside own network) but also the thorough understanding of the scale of the effects (temporary or reversible impact, permanent or

destructive impact) (Hoffman and Nyikos 2018: 57; on the benefits and problems connected to different active cyber-defence tools, see for example Jarko 2016). The considerations implied in choosing to consciously apply such defensive measures should not be the responsibility of a company's security person or team but should be a policy decision backed up by the management and taken in consultation with the right experts and in view of the relevant legislation. Finally, we should accept that no security technology is perfect, and as long as there are security measures there will be cyber criminals calculating ways to evade them.

References

Anonymous (2018) APT10 was managed by the Tianjin bureau of the Chinese Ministry of State Security. Intrusion Truth. https://intrusiontruth.wordpress.com/2018/08/15/apt10-was-managed-by-the-tianjin-bureau-of-the-chinese-ministry-of-state-security/. Last access 7 July 2019

Brunoni L (2016) Private cyberwars and the right to hack back. Jusletter. https://jusletter.weblaw.ch/juslissues/2016/872/private-cyberwars-an_d13bbca261.html__ONCE. Last access 7 July 2019

Denning DE, Strawser BJ (2017) Active cyber defence: applying air defence to the cyber domain. Carnegie Endowment for International Peace https://carnegieendowment.org/2017/10/16/active-cyber-defence-applying-air-defence-to-cyber-domain-pub-73416. Last access 7 July 2019

Dewar R (2017) Active cyber defence. Research Gate. https://www.researchgate.net/profile/Robert_Dewar5/publication/321057804_Active_Cyber_Defence/links/5a0af4570f7e9b0cc024f3c2/Active-Cyber-defence.pdf?origin=publication_detail. Last access 7 July 2019

Dittrich D, Himma KE (2005) Active response to computer intrusions. In: Handbook of information security 3. Wiley, New Jersey, pp 664–681. https://staff.washington.edu/dittrich/misc/handbook-arc.pdf. Last access 7 July 2019

Fletcher GP (1989) Punishment and self-defence. Law Philos 8(2):201–215

Hessbruegge JA (2017) Human rights and personal self-defence in international law. Oxford University Press, New York

Himma KE (2004) The ethics of tracing hacker attacks through the machines of innocent persons. Int J Info Ethics 2(11):1–13

Hoffman W, Nyikos S (2018) Governing private sector self-help in cyberspace: analogies from the physical world. Carnegie Endowment for International Peace. https://carnegieendowment.org/2018/12/06/governing-private-sector-self-help-in-cyberspace-analogies-from-physical-world-pub-77832. Last access 7 July 2019

Jarko C (2016) Finding the fine line – taking an active defence posture in cyberspace without breaking the law or ruining an enterprise's reputation. SANS Institute. https://www.sans.org/reading-room/whitepapers/legal/finding-fine-line-%E2%80%93-active-defence-posture-cyberspace-breaking-law-36807. Last access: 7 July 2019

Lin P (2016) Ethics of hacking back. Ethics + Emerging Sciences Group. ethics.calpoly.edu/hackingback.pdf. Last access 7 July 2019

Niggli M, Göhlich C (2019a) Art. 15 – Rechtfertigende Notwehr. In: Basler Kommentar, Strafrecht I, 4. Helbling Lichtenhahn Verlag, Aufl., Basel, pp 249–260

Niggli M, Göhlich C (2019b) Art. 17 – Rechtfertigender Notstand. In: Basler Kommentar, Strafrecht I, 4. Helbling Lichtenhahn Verlag, Aufl., Basel, pp 265–271

Rabkin J, Rabkin A (2016) Hacking back without cracking up, A Hoover Institution essay. Aegis Paper Series 1606. https://www.hoover.org/sites/default/files/research/docs/rabkin_webreadypdf.pdf. Last access 7 July 2019

Rid T, Buchanan B (2015) Attributing cyber attacks. J Strategic Stud 38(1–2):4–37
Schmidle N (2018) The digital vigilantes who hack back. The New Yorker. https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back. Last access: 7 July 2019
Smolanoff JN, Brill A (2018) Hacking back against cyberterrorists – risks & benefits analysis for NATO's COE-DAT. Kroll. https://www.kroll.com/en/insights/publications/cyber/hacking-back-against-cyberterrorists. Last access: 7 July 2019
Stevens S (2019) Do we need a new paradigm of self-defence for cyberspace? In: Dal Molin-Känzlin A, Schneuwly AM, Stojanovic J Digitalisierung - Gesellschaft - Recht, Analysen und Perspektiven von Assistierenden des Rechtswissenschaftlichen Instituts der Universität Zürich, DIKE, Zürich/St.Gallen, pp 323–340
Swinhoe D (2018) US 'hacking back' law could create a cyber wild west of vigilantism. IDG Connect. https://www.idgconnect.com/abstract/29246/us-hacking-law-create-cyber-wild-west-vigilantism. Last access: 7 July 2019
Volokh E (2007) The rhetoric of opposition to self-help. Volokh Conspiracy. http://www.volokh.com/posts/1176319370.shtml. Last access: 7 July 2019