Journal of Universal Computer Science, vol. 24, no. 5 (2018), 646-661
submitted: 23/1/18, accepted: 28/4/18, appeared: 28/4/18 © J.UCS

Obligation to Defend the Critical Infrastructure? Offensive Cybersecurity Measures

Anže Mihelič
(Faculty of Law, University of Ljubljana, Slovenia
mihelic.anze@gmail.com)

Simon Vrhovec
(Faculty of Criminal Justice and Security, University of Maribor, Slovenia
simon.vrhovec@fvv.uni-mb.si)

Abstract: Critical infrastructure is vital for the functioning of the state and the society. Even though the legal foundations for critical infrastructure protection in material world are well-established, there is almost no legal basis for providing critical infrastructure security in the cyberspace. In this paper, we study the applicability of different types of cybersecurity measures including the most offensive ones in different domains by drawing parallels to providing security in the material world. By further focusing on the offensive cybersecurity measures (i.e., hack back), we lay out the circumstances in which such invasive measures could be employed for providing security for the critical infrastructure.

Keywords: Hack back, Private security, Critical infrastructure protection, Offensive cybersecurity
Categories: K.4.1, K.5, K.5.2, K.6.5

1 Introduction

Critical infrastructure systems are among the most data intensive and sensitive. Their primary function is to provide the vital capacity to the state and the society. The attribution of the term *critical infrastructure* has not been uniform and consistent throughout history. At first, infrastructure was considered critical only if a lasting disruption caused military or economic disturbances [Patrascu and Simion 2014]. Today, critical infrastructure is expanding to various other areas of societal life [Auerswald, Branscomb, La Porte and Michel-Kerjan 2005]. Some authors have even indicated that it is becoming increasingly hard to identify sectors that are not considered as critical [Lewis 2006]. Since the critical infrastructure on both conceptual and operational levels came into focus only after a rise in the perceived terrorism threat [Prezelj et al. 2008], the critical infrastructure systems may be defined according to the degree of paralysis of society and state that a failure of the critical infrastructure system would cause. The dependence of the society on the critical infrastructure therefore presents a tempting choice for terrorist and other typically organized attackers (e.g., hacktivists, nation states, crime organizations). The state and critical infrastructure operators are often faced with new types of attacks, especially regarding the attacks from the cyberspace [Boin, Lagadec, Michel-Kerjan and Overdijk 2003].

Primarily, it is a responsibility of the state to provide the highest level of critical infrastructure protection [Prezelj et al. 2008]. The direct implementation of security measures, both in the material world and in the cyberspace, to achieve a defined set of security objectives is however mostly in the hands of the critical infrastructure operators themselves [Auerswald et al. 2005]. The provision of critical infrastructure services is inherently related to the use of information and communication technology thus making critical infrastructure complex cyber-physical systems [Lukman and Bernik 2008]. The difficulty of ensuring adequate levels of cybersecurity for these systems is however exponentially correlated with their complexity [Mihelič and Vrhovec 2017]. Often transnational threats to the critical infrastructure need immediate and effective mitigation otherwise they may significantly affect other systems that are depending on the critical infrastructure. Following the findings that a modern society is becoming increasingly vulnerable [Boin et al. 2003], the critical infrastructure operators need an adequate legal and expert support that would enable them to successfully protect the critical infrastructure and consequently the society as its users.

The transformation of relatively rigid legal systems to a legal system that is capable of adequately adapting to the fast pace of technological progress is undoubtfully the biggest challenge of legal systems in the information age. For example, the European Union (EU) adopted the Directive on security of network and information systems (NIS Directive) in 2016 to provide the legal measures to boost the overall level of cybersecurity in the EU. The EU member states must implement it in their national legislation (e.g., Slovenia is in the process of adopting the Act on information security) and identify the operators of essential services in 2018. Despite the effort of the EU and its member states to establish an adequate system for the implementation of defensive, preventive, repressive and curative measures on the state level, member states are often facing threats in the cyberspace that require real-time cybersecurity measures. The EU member states however currently do not have an appropriate and uniform legal basis to confront these cyberthreats.

The information and communication technology progress enabled new threats that can paralyze individual organizations but also whole parts of the society. These cyberthreats require specialized mitigating approaches on the national level in terms of preventing, detecting, investigation and prosecuting such malicious acts. Also, key actors need state support, adequately educated and trained personnel, and legislation adapted to specific circumstances.

In this paper, we focus on the legal aspects of ensuring the cybersecurity of critical infrastructure operators. The paper studies the applicability of different types of cybersecurity measures (i.e., preventive measures, collecting intelligence, blockade and neutralization) in different domains (i.e., organizational network, public network and apparent attack sources). We will also draw parallels with security services in the material world to justify the need or a lack of need for specific types of cybersecurity measures including the most offensive ones.

The paper is structured as follows. In the next section, we lay the conceptual grounds for providing security in the cyberspace by determining the limits of the cyberspace and analyze different cybersecurity measures at disposal in different domains. Next, we present the critical infrastructure protection in the material world and consider the applicability of the material world concepts to the cyberspace.

Finally, we present the offensive critical infrastructure cybersecurity by drawing analogies to the material world and conclude the paper with some final remarks.

2 Cybersecurity measures

"*The progress of science in furnishing the Government with means of espionage is not likely to stop [with wiretapping]. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home*" [Brandeis 1928]. These 'prophetic' words on the impact of technology development on our privacy written by one of the greatest legal minds in our history Louis Brandeis in his dissenting opinion in the first documented case of telephone tapping. The development of technology made Brandeis predictions possible – due to current technological advances it could be even said that these predictions are exceeded [Mihelič, Bernik, Markelj and Zgaga 2017].

2.1 Limits of the cyberspace

Cybercrime does not follow a general decline in conventional material world crime in the Western countries [Friedman, Grawert and Cullen 2017, Pool and Custers 2017, van Dijk, Tseloni and Farrel 2012]. The emergence and explosion of global connectivity have led to a steady growth of a relatively new types of crimes that takes place in an invisible and intangible place, namely the cyberspace, whose territorial boundaries are almost impossible to determine, and in which both individuals and organized groups act to achieve personal, ideological, economic or security gain [Abel and Schafer 2011, Halavais 2000, Jiménez, Orenes and Puente 2010, Johnson and Post 1996, Malby et al. 2013]. Although cybercrime is often associated with individual computer enthusiasts, up to 80 percent of cybercrime is related to some kind of organized activity [Malby et al. 2013].

Successful prevention of organized cybercrime which is only partially taking place in the material world requires looking beyond the usually well-defined national borders that delineate where specific legislations apply. When dealing with criminal activities in the material world, geographical interpretation of national borders is usually sufficient since physical crime scenes cannot travel easily [Abel and Schafer 2011]. The cyberspace however introduces the need for different understanding of the space itself as it appears to be both infinite and infinitesimal, i.e., everything is at a hand's reach and there is potential for infinite possible interactions and information that grows exponentially [Jiménez et al. 2010]. This raises the issue of place existence in the cyberspace with some authors claiming that *placeness* does exist in the cyberspace. Even though it is impossible to accidentally stray across the border into cyberspace [Johnson and Post 1996], physical location in the material world remains vitally important for the legal systems as we know them to work.

The cyberspace both undermines and transforms the components of time and space [Kerstens and Veenstra 2015]. Likely offenders may attack continuously and multiple victims at the same time remotely, i.e., without the physical presence at the location of victims' systems or the victims themselves [Yar 2005, Završnik 2013]. Offenders can attack from almost anywhere in the world often through compromised

devices of secondary victims who are unaware of their role in a cyberattack. Criminal acts in the cyberspace can thus persists as long as victim is connected to it [Hinduja and Patchin 2010]. The use of anonymization technologies and tools, such as the TOR network and its hidden services, seem to make attackers extremely difficult to identify thus making criminal investigations for the law enforcement authorities nearly impossible provided they are using traditional investigative measures.

The understanding and acceptance of the mentioned specifics of the cyberspace compared to the material world is crucial for providing adequate critical infrastructure protection and protection of other areas of corporate and national security. International cooperation and active monitoring of technology development is almost unconditionally required due to the internationality of the cyberspace and quick adaptations to new technologies by attackers in the cyberspace.

2.2 Cybersecurity measures

Cybersecurity measures can be classified in various ways. In this paper, we first classify cybersecurity measures according to their purpose: preventive measures, collecting intelligence, blockade and neutralization. *Preventive measures* encompass all measures, either technical, social, organizational, legal etc., that are aiming at boosting the security of a protected system, e.g., an organizational network and its devices. For example, it includes training and raising awareness, routine updating and patching systems, adopting information security policies, sharing virus signatures etc. The purpose of *collecting intelligence* is to gather information about cyberattacks to return private property or to report to the authorities. Intelligence can be collected from various logs, by network monitoring, analyzing malware etc. It can be also collected by more invasive measures, such as installing remote forensic software or spyware. *Blockade* refers to any kind of blocking the potential/apparent attacker by blocking potential attack vectors (e.g., with a firewall), blocking all network traffic to apparent sources of a cyberattack. The final type of cybersecurity measures *neutralization* is the most invasive and results in the incapability of the apparent attacker to continue the cyberattack. Neutralization may have different purposes, from searching for and wiping stolen data to remote overtakes of command and control (C&C) servers.

The same cybersecurity measure can technically fit into different classes based on the purpose of their implementation. For example, setting up a firewall may be considered as a preventive measure. However, if the firewall is adapted to block a potential attacker in real-time, then this is considered a blocking measure. Similarly, regular patching may be considered as a preventive measure. However, patching may be considered as a blocking measure if it is applied to fix a vulnerability targeted by an attacker. If this patch is permanent, then it is also a preventive measure preventing future similar attacks.

The presented classification of cybersecurity measures has its merits however it seems limiting as it does not provide any insight into the different domains in which cybersecurity measures may act which is an important aspect in any legal context. We thus further divide cybersecurity measures according to the enacting domain, i.e., the context in which they are employed. Figure 1 presents the three relevant domains: organizational network, public network and apparent attack sources.

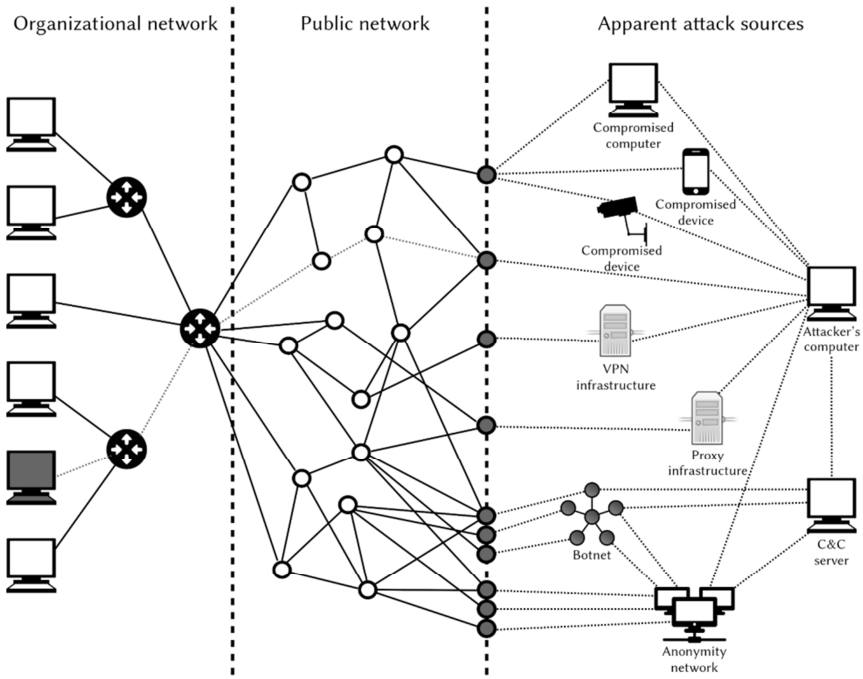

Figure 1: Domains in the cyberspace

The *organizational network* domain encompasses all network infrastructure and connected devices owned or operated by a defending organization. It is usually physically separated from the public network (e.g., internet) unless a VPN infrastructure is in place. In the organizational network, the legislation is the least restrictive and the organization has the most control over the residing devices. In the organizational network, all four types of cybersecurity measures apply: preventive measures (e.g., employee training, using strong passwords, routine updating and patching of computer systems, using honeypots), collecting intelligence (e.g., analyzing logs, network monitoring, collecting and analyzing malware samples, determining established connections), blockade (e.g., using firewalls, anti-malware software, access control) and neutralization (e.g., removing malware from a compromised device in the organizational network). The most restrictive is the right for privacy which makes it hard to collect evidence from employees' computers in case of an internal attacker.

The *public network* domain is the cyberspace between the defending organization and the apparent attacking source. The defending organization usually does not have any control over the devices in the public network. Also, the legislation is much more restrictive in the public network as the devices are owned by others. The cybersecurity measures that the defending organization can employ are mostly restricted to preventive measures (e.g., choosing the internet service provider and security package) and collecting intelligence (e.g., passive gathering information on

the attackers, open source intelligence – OSINT). Even if the defending organization does not have control over the devices in the public network, they may still use security services provided by internet service providers (ISP), law enforcement agencies and CERTs. These services include three types of cybersecurity measures: preventive measures (e.g., sharing malware signatures, contractual obligations of service subscribers), collecting intelligence (e.g., network monitoring, blacklisting devices with malicious activity) and blocking (e.g., disconnecting a malicious device from the public network). Since the public network does not include the apparent attack sources, it is not possible to neutralize them in this domain.

The *apparent attack sources* domain is the attacker infrastructure and can range from very simple (e.g., only the computer of the attacker without intermediaries) to very complex settings (e.g., botnet that uses the TOR network for attacking the organization and communicating with the C&C servers while the attacker connects to a C&C server through a few proxy servers). Measures in this domain are offensive cybersecurity measures that commonly referred to as 'hack back' as it involves a varying degree of hacking the apparent attack sources. This form of self-defense has been often heavily criticized by the public [Iasiello 2014, Kallberg 2015, McGraw 2013, Messerschmidt 2013, Pool and Custers 2017]. McGraw writes »*The last thing we need in computer security is a bunch of vigilante yoo-hoos and lynch mobs*« and adds that a possible legalization of the hack back would be irresponsible and a recipe for a disaster [McGraw 2013]. As it is a very invasive measure that could cause a chaotic and uncontrollable situation in the cyberspace, it must not be taken lightly and allow its implementation to anyone and anytime. Arbitrary use of some forms of counter-attacks, such as physical force, coercive means and firearms, by the state or private security companies would lead to a chaotical situation in the material world and a similar situation would be reached by nonregulated and arbitrary use of offensive cybersecurity measures. Nevertheless, it cannot be completely overlooked due to its potential effectiveness. As already mentioned, neither defending organizations, state authorities nor private security companies have such legal powers. Nevertheless, we will analyze the benefits and limitations of such cybersecurity measures. The potential benefit and limitation of an offensive cybersecurity measure varies greatly depending on the type of apparent attack source.

In the simplest case, the apparent attack source is the attacker's own computer. In this case, all types of cybersecurity measures would be applicable: preventive measures (e.g., installing a backdoor for easy access in case the attacker decide to attack again, installation of malware that neutralizes the attacker's computer in case of an attack), collecting intelligence (e.g., searching for stolen data, collecting digital evidence, network monitoring, determining the habits of the attacker), blockade (e.g., blocking all traffic to the defending network) and neutralization (e.g., destruction of stolen data, disruption and incapacitation of an ongoing cyberattack).

This is however usually not the case as the attacks are commonly done through a compromised system (e.g., computer, device) of an unaware third party. All cybersecurity measures are therefore applicable like in the case of the attacker's computer however the possibility of secondary victimization cannot be ignored. For example, determining the habits or monitoring the browsing activity of a home computer owner would be an unfounded invasion of the device owner's privacy.

Detection of the type of the apparent attack source and restrain from some measures are therefore required.

In recent years, botnets have formed from a vast number of compromised devices which was made possible especially by the lack of security features in IoT devices due to the cycle of blame, i.e., each stakeholder involved in a product life-cycle blames the other stakeholders for the lack of and for not fostering the improvement of security features [Wendzel and Kasem-Madani 2016]. If classical hacking techniques can easily be employed in the first two cases, they do not seem to be scalable to the large number of devices that comprise a botnet. For example, blocking or neutralizing devices in the botnet one by one during an ongoing cyberattack just does not make any sense. Botnets are controlled by C&C servers therefore the primary target of an invasive cybersecurity measure would be determining it (e.g., by monitoring the network, analyzing malware). Preventive measures are also possible. For example, forming anti-botnets (i.e., botnets with a legally authorized operator) could quite swiftly neutralize an attack from a botnet or significantly diminish its impact depending on the size of the intersection between both botnets.

Things get much more complex if the attacker uses proxy servers, VPN infrastructure or anonymity networks (or any combination of those). In all these cases, the apparent attacker is just a public (e.g., TOR network, public proxy server) or private (e.g., VPN infrastructure, private proxy server) network node that most often does not have any relation with the malware used for the cyberattack or the attacker himself. Since the attacker is not the only one who is using these nodes, it becomes increasingly difficult to either block or neutralize them. For example, if a lot of attacks are coming from a TOR exit node, it could be neutralized remotely. This would have little to no impact on the cyberattack as the TOR network is designed to automatically adapt to changes in its network and would just use other exit nodes instead. In addition, the neutralized exit node could easily be operated by the authorities as states are widely believed to control TOR exit nodes in an effort to deanonymize its traffic. There are similar issues with VPN and proxy servers. Just by using an intermediary, the truly applicable cybersecurity measures would be reduced to preventive measures (e.g., inducing malware into the aforementioned infrastructure) and collecting intelligence (e.g., determine the next apparent attack source). The use of the TOR network or other anonymity networks would effectively diminish the usefulness of the invasive cybersecurity measures to close to zero. Nevertheless, the use of VPN and proxy servers by the attacker may make it easier to trace them as these connections tend to be significantly less dynamic.

Apparent attack sources may be found in the organizational network as well. There is little difference between apparent attack sources in the public and the organizational network. For example, in the organizational network, one can find the attacker's computer in case of an internal attacker and compromised devices that may be controlled by the attacker from either the organizational or the public network. In cases of big organizational networks with a considerable number of compromised devices, miniature organizational botnets may form whose C&C servers may reside in any of the two networks.

3 Critical infrastructure protection in the material world

Security is an increasingly cherished and protected fundamental human good and is one of the constitutionally protected human rights (Constitution of the Republic of Slovenia, Article 34 (Official Gazette RS Nos. 33/91-I, 42/97, 66/2000, 24/03, 69/04, 68/06, and 47/13)) that protects it from both interference by the state authorities and individuals alike [Šturm 2002]. It is a fundamental human value and a precondition for the existence and development of the society thus it is primarily and traditionally provided by the national security system of the state (e.g., army, internal security, protection and rescue) [Sotlar and Čas 2011]. Providing a high degree of internal security is not in the exclusive authority of the police as private security actors, such as private security companies and personal detectives, may also contribute to the security of people and property. These actors protect people and their property from theft, damages, destruction and other forms of harmful activity for a price and are legally regulated economic activities due to their legal admissibility of interference with the human rights and fundamental freedoms of individuals.

The right to interfere with the most fundamental human rights and freedoms guaranteed and protected by the constitution was only a few decades ago an exclusive right of the police. Today, interference with these rights by the private organizations is becoming a reality at every step. Private security companies often work in public spaces, such as airports, shopping centers, entrances to office buildings, resort centers etc. [Button 2003, Wakefield 2008], and yet they act in the private interest as their scope of work in protected area is based on a contractual relationship [Loyens 2009] and beyond the traditional concepts of self-defense. This is a privatization of the security sector which is commonly referred to as *rent-a-cop*. Different legal systems are allocating different powers to the security guards. For example, security guards in South Korea are not allowed to exercise any powers that would exceed the powers of any citizen [Button and Park 2009]. In South Africa, security guards are dressed in uniforms that are similar to police uniforms, almost all of them are equipped with automatic or semi-automatic weapons and are allocated the same powers as the police [Singh and Kempa 2007].

In Slovenia, the security personnel have some statutory powers however their scope is narrower compared to police powers. The law in Slovenia determines the forms of protection, the powers of the security guards (the Slovenian legislation refers to *powers* as *measures*) and the conditions under which the powers may be used [*Zakon o zasebnem varovanju (ZZasV-1)* 2011]. According to the Slovenian legislation, security personnel can restrict and interfere with constitutionally protected human rights on a protected area by using physical force. Under certain conditions related to preventing threats to people and property or immediate and unlawful assault that endangers the security guard's own life or the life of a person under protection, security personnel can use coercive measures that are confined to a service dog (only for threat detection), handcuffs and other means of restraint, incapacitating spray and weapons (namely, firearms).

In some cases, the provision of security is not only a right but also an obligation. The provision of private security in Slovenia is therefore not exclusively left to the decisions of organizations, state authorities and other institutions. In cases when an entity is performing an activity where there is a predictable possibility of unexpected

danger or increased level of security risk to the safety of people, nature or property, the law requires the obligatory provision of security. These cases are mostly related to entities that archive material and objects representing the cultural heritage, store or use substances and devices hazardous to people and the environment, public events organizers, entities that manage large amounts of cash or securities, critical infrastructure operators or when protection is necessary for special security reasons.

The presented powers of private security guards, permissibility of the use of force and coercive measures that security guards can employ and the existence of the legal concept of obligatory provision of security in cases and under conditions as defined by national legislations indicate a recognition of the state that its national security system alone is insufficient for provisioning security to people and property. In the material world, private security is therefore playing an important role in protecting the critical infrastructure whose quality and integral protection is in the public interest. With the increasing use of the cyberspace, there is an inevitable increase in the need to protect the critical infrastructure from increasingly frequent and invasive cyberthreats.

4 Applicability of the material world concepts to the cyberspace

Cyberattacks are becoming increasingly numerous and invasive. The fight against them is fundamentally asymmetric and favoring the attackers [Miraglia and Casenove 2016]. *Stuxnet*, *Flame*, *Equation*, *Duqu* and *Night Dragon* are only a few names that require special attention when discussing the importance of cybersecurity, the severity of damages due to cyberattacks and the difficulty of defense against them [Miller and Rowe 2012].

It is generally considered that the state has the exclusive right to use force and to interfere with human rights. In cases when the state is not able to provide adequate protection, the state recognizes the legal and moral right of legal entities to defend themselves. In a way, the state protects constitutionally guaranteed rights with their negation [Bavcon 1997]. The transfer of the right to use force may be reflected in a transfer of a public authority to private subjects, such as security companies, or exclusion of the unlawfulness of acts that have otherwise all the signs of criminal offenses (e.g., acting in self-defense, coercion). These legal concepts are intended for situations when two legal goods collide. In this case, the legal good that has less importance in a certain situation must be withdrawn [Bavcon and Šelih 2003].

The use of self-defense in the cyberspace is somewhat more complicated. Most modern legislations exclude the unlawfulness or at least the criminality of acts in the material world that have all the signs of criminal offenses but are committed in special circumstances. For example, in Slovenia, an act that has all the signs of a criminal offense is not unlawful if it has been committed to discourage a concomitant unlawful attack on oneself, someone else or in some cases on property [Zgaga 2011].

Legal concepts for the exclusion of legal responsibility for offenses that apply to the material world can analogously be applied to the cyberspace. Certainly, the owner of a compromised device causing a cyberattack cannot be responsible for a criminal offense even if there is a causal link between the use of the device and the cyberattack (e.g., the owner physically connected the device to the cyberspace and managed it), the device was not adequately protected and the owner does not prevent the offense

because he is not aware of the presence of malware on his device and its role in the cyberattack. Likewise, someone who cannot prevent the cyberattack because his device has been blocked by malware, cannot be held responsible for a criminal offense.

The legal admissibility of self-defense, the right and in certain cases the obligation of legal subjects to organize private security for protecting people and property, and the national security system constitute a robust system that guarantees the highest level of security for legal entities in the material world in Slovenia. It is however different in the cyberspace. Despite the adoption of new measures both on the level of the European Union (e.g., proposal for an EU Cybersecurity Agency, new European certification scheme ['State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks' 2017]) as well as on the level of individual states, there is no adequate legal basis for offensive defense in the vast majority of legislations even though this idea is not new [Jayawal, Yurcik and Doss 2002, Lin 2016].

Self-defense of organizations in the cyberspace is somewhat more complicated than in the material world. In the material world, organizations can hire private security companies which can help with providing a higher level of security. Security guards in the private security sector are in many countries allowed to interfere with fundamental human rights to defend property in the guarded area. In Slovenia, for example, private security guards can use various (*numerus clausus*) security measures, even physical force and firearms in situations specified by law. These measures can be used beyond the narrow limits of the traditional self-defense concept to protect people and property in a protected area. These measures are however limited to the material world and therefore providing security in the cyberspace needs to rely solely on the traditional legal concepts of self-defense.

These findings suggest a paradoxical situation. Private security companies today often help provide security in primary and secondary schools with technical (e.g., video surveillance) and physical security services. These services are primarily intended to protect the students from external threats however the schools recognize the need for security guards due to the increasing frequency of vandalism and violence [Lorenčič 2003]. In this case, a private security system is established in areas frequented by minors to protect people and property. This system is designed to exceed the arising threats and as such acts also preventively and repressively. Security guards can thus use their legal powers in the protected area including the use of force to interfere with the rights of students and other people to protect people and property. From the admissibility of this form of security it is possible to conclude that on one hand the state permits in increasingly intense restriction of human rights by the private sector (e.g., video surveillance in sanitary facilities, such as toilets [Lorenčič 2003]) to protect the minors. On the other hand, the state admits that the minors constitute a sufficient security problem for people and property to justify external protection by private security companies. The equipment and the powers of the security guards in schools do not remain unchanged with the increasing threats. In some schools in the USA, school security guards and even some school employees are armed due to shooting hikes by students [Flock 2013].

The aforementioned example is used as *reductio ad absurdum*. Protection of people and property is optional since organizations can decide for themselves if

external security services are needed or not and in which form [Lorenčič 2003]. As already mentioned, it is legally stipulated to organize private security for the critical infrastructure in Slovenia only where security is limited to the material world. Critical infrastructure operators in Slovenia therefore find themselves in a situation where the legislation does not provide an unambiguous legal basis for effective and necessary defense in the cyberspace which would be adapted to the most advanced threats. Thus, at present, the legal admissibility of offensive security measures can be sought only in the legal institute of self-defense, but due to the particularity of the cyber space it offers only limited possibilities of argumentation.

5 Offensive critical infrastructure cybersecurity

There is always a sense of helplessness in ensuring security in the cyberspace [Lin 2016] since the state is not capable to offer help comparable to the help provided in the material world. Due to this, most of the responsibility for protection lies on the potential victim which is either a natural or legal person.

Counter-attacks in the cyberspace interfere with the constitutionally guaranteed human rights and can therefore be used only when the goal of their use is constitutionally admissible and legitimate, and the employed measures absolutely necessary, appropriate and proportionate. The Netherlands made the first steps towards the legalization of offensive cybersecurity measures with a proposal on the Act on Cybercrime that would allow state authorities to hack into computers (‘hacking back’), to install spyware and to destroy or disable access to files with the ‘notice and take down’ order [Pool and Custers 2017]. Negotiations on the enactment of hack back are also taking place in Germany where such changes require amendments to the constitution [Mpoke Bigg 2017].

5.1 Direction toward the source

An act to protect people or property that has all the signs of a criminal offense can be designated as not unlawful or decriminalized only if it is directed towards the attacker [Bavcon and Šelih 2003]. This is a crucial element of self-defense that is frequently questioned in the cyberspace as it is hard to determine who the attacker is and how to make a successful identification [McGraw 2013]. Incorrect identification of the attacker is not uncommon [Jayawal et al. 2002] and could lead to damaging systems not directly involved in the cyberattack. Therefore, it would make sense to first employ offensive measures to determine whether the apparent attack source is the attacker’s or a compromised device. It is significantly more difficult to determine the identity of an attacker if he is using VPNs, proxy servers or anonymity networks at any point between the real attacker and the attacked system as they form a public or private network infrastructure and can be used by a variety of others that have no relation to the cyberattack. Although the TOR network provides a certain level of anonymity, several deanonymization techniques that leverage traffic correlation attacks, electronic fingerprinting, operational security failures, and remote code execution exist [Nurmi and Niemelä 2017]. There is also a possibility of gaining some intelligence on the attacker from VPN operators and proxy servers. This however creates a problem as collecting intelligence about the attacker would require the use of

offensive measures (e.g., with the use of remote forensic software) against targets that are clearly not directly related to the cyberattack.

5.2 Concomitance and unavoidability

We often speak of offensive cybersecurity measures when a particular threat directed towards a specific target (i.e., a critical infrastructure operator) needs urgent and immediate attention to dissuade it. This implies that it would not be possible to discourage the cyberattack or prevent its consequences in any other way. Anyone can act against an unlawful attack on himself or someone else. A private security guard can interfere with someone's fundamental rights in accordance with his legal powers in a protected area if the objective of employing a certain measure could not be achieved by less restrictive measures.

The interpretation of concomitance is more difficult in the cyberspace then in the material world. Concomitance may thus be understood somewhat differently as hacking requires a significant investment of time making it hard to determine when the attack started and when it ended (if it ended) due to the difficulty of determining if the attack is still on-going. Intrusions may remain unnoticed for months or even years and after their identification and neutralization it is still hard to determine if the attack has been fully stopped. A particular challenge are repetitive attacks where individual cyberattacks could be only peaks of a major cyberattack campaign. Determining concomitance is also an issue in data theft. The tracking and seizure of stolen data can practically be carried out only after the act of data theft has ended. Such attacks may appear to last only a few seconds or minutes. It is however unclear for how long the attack really took place before the data theft and if and for how long the attack continues after it. Again, the attack may be a part of a larger-scale attack on the critical infrastructure.

5.3 Proportionality

Concomitance and unavoidability raise the question whether defense could be allowed against an attack that has not yet started but it could be expected (e.g., by setting up traps that can damage the attacker once he starts the attack – a cyber minefield). Even though there is no definite answer to this question, it is worth looking for an answer in the proportionality between the intensity of the attack and the defense [Bavcon and Šelih 2003]. It is not and cannot be allowed that anyone can protect their interests in full force, by any means and at any cost [Bavcon and Šelih 2003]. Thus, it is permissible to employ only those measures that result in damage that does not exceed the benefits obtained by such defense [Denning 2014] whereby this is more about an assessment of the appropriate extent and type of defense necessary to deter the attack than just weighing the equivalency of the goods [Bavcon and Šelih 2003].

The assessment of proportionality is the subject of any discussion on offensive cybersecurity measures since defense should be limited to urgently needed measures that effectively protect people and property with the mildest human rights interferences. When performing a hack back, the security personnel employing it could inadvertently compromise devices that are not directly involved in the cyberattack or seize data that was not originally acquired by the cyberattack. The

question of proportionality is therefore inevitably extended to the question of the extent of the collateral damage that such an attack can cause. The defender may even be unaware or not willing to be aware regarding to this issue.

The cyberspace may have become a battleground of various attackers and counter-attackers. It is thus necessary to build awareness that more and more subjects with different relationships are entering this cyber-battlefield. With a counter-attack protecting one system may endanger another that is not related to the original cyberattack. In such cases, the defender may unintentionally become the attacker. In general, just because a victim hacks back an attacker it does not make it any less of a crime in the eyes of the law [Jayawal et al. 2002]. Therefore, offensive cybersecurity measures that target a presumed attack source must be applied carefully, especially if they can cause damage, such as blocking and neutralization that affect the availability and integrity of data and systems [Denning 2014].

6 Conclusion

This paper presents a simplified outline of two highly complex scientific fields with the purpose of improving mutual understanding and building common foundations which can enable the search for the most suitable solutions to protect the social reality from various forms of threats that arise in the cyberspace. Use of offensive cybersecurity measures is currently not legally admissible in most countries. In accordance with the principle of the rule of law, any state interference with fundamental human rights of the individual must be statutory regulated since the state is not allowed to act unless expressly permitted. Only when the state would have these powers itself, it could confer these powers to private actors (e.g., private cybersecurity companies) who could operate in the cases and under the conditions expressly laid down by law. Thus, this area remains mostly statutory unregulated and consequently not admissible. The state should take a view on this urgent need for such measures and consequently interference with human rights of attackers and those representing the possible collateral damage and adopt such statutory rules which would precisely determine who, when and under what conditions those rules can be implemented. With this we could at least partly avoid a complete disorder in this field and thus the arbitrariness of the use of offensive cybersecurity countermeasures.

References

[Abel and Schafer 2011] Abel, W., Schafer: ‘Big Browser Manning the Thin Blue Line - Computational Legal Theory Meets Law Enforcement’; Problema, Vol. 2 (2011), pp. 51–84. https://doi.org/10.22201/iij.24487937e.2008.2.8048

[Auerswald, Branscomb, La Porte and Michel-Kerjan 2005] Auerswald, P., Branscomb, L. M., La Porte, T. M., Michel-Kerjan, E.: ‘The challenge of protecting critical infrastructure’; Issues in Science and Technology, Vol. 22, No. 1 (2005), pp. 77–83.

[Bavcon 1997] Bavcon, L.: ‘Kazenskopravno varovanje človekovih pravic in temeljnih svoboščin’; In M. Pavčnik, A. Polajnar-Pavčnik & D. Wedam-Lukić (Eds.), Temeljne pravice. Ljubljana: Cankarjeva založba (1997), pp. 406–439.

[Bavcon and Šelih 2003] Bavcon, L., Šelih, A.: 'Kazensko pravo. Splošni del'; Ljubljana: Uradni list Republike Slovenije (2003).

[Boin, Lagadec, Michel-Kerjan and Overdijk 2003] Boin, A., Lagadec, P., Michel-Kerjan, E., Overdijk, W.: 'Critical Infrastructures under Threat : Learning from the Anthrax Scare'; Journal of Contigencies and Crisis Management, Vol. 11, No. 3 (2003), pp. 99–105.

[Brandeis 1928] Brandeis, L.: 'Dissenting opinion of Justice Louis D. Brandeis in Olmstead v. United States'; (1928).

[Button 2003] Button, M.: 'Private security and the policing of quasi-public space'; (2003). https://doi.org/10.1016/j.ijsl.2003.09.001

[Button and Park 2009] Button, M., Park, H.: 'Security officers and the policing of private space in South Korea: profile, powers and occupational hazards'; Policing and Society, Vol. 19, No. 3 (2009), pp. 247–262. https://doi.org/10.1080/10439460903145668

[Denning 2014] Denning, D. E.: 'Framework and principles for active cyber defense'; Computers and Security, Vol. 40 (2014), pp. 108–113. https://doi.org/10.1016/j.cose.2013.11.004

[Flock 2013] Flock, E.: 'At Least 7 States Now Have Armed Staff in Schools'; (2013).

[Friedman, Grawert and Cullen 2017] Friedman, M., Grawert, A. C., Cullen, J.: 'Crime Trends: 1990-2016'; (2017).

[Halavais 2000] Halavais, A.: 'National Borders on the World Wide Web'; New Media & Society, Vol. 2, No. 1 (2000), pp. 7–28. https://doi.org/10.1177/14614440022225689

[Hinduja and Patchin 2010] Hinduja, S., Patchin, J. W.: 'Bullying, Cyberbullying, and Suicide'; Archives of Suicide Research, Vol. 14 (2010), pp. 206–221. https://doi.org/10.1080/13811118.2010.494133

[Iasiello 2014] Iasiello, E.: 'Hacking Back: Not the Right Solution'; Parameters, Vol. 44, No. 3 (2014), pp. 105–113.

[Jayawal, Yurcik and Doss 2002] Jayawal, V., Yurcik, W., Doss, D.: 'Internet Hack Back : Counter Attacks as Self-Defense or Vigilantism ?'; In IEEE International Symposium on Technology and Society (ISTAS). Raleigh NC (2002), pp. 380–386.

[Jiménez, Orenes and Puente 2010] Jiménez, A. G., Orenes, P. B., Puente, S. N.: 'An Approach to the Concept of a Virtual Border: Identities and Communication Spaces.'; Revista Latina de Comunicación Social, Vol. 13 (2010), pp. 1–8. https://doi.org/10.4185/RLCS-65-2010-894-214-221-EN

[Johnson and Post 1996] Johnson, D. R., Post, D.: 'Law and borders: The rise of law in cyberspace'; First Monday, Vol. 1, No. 1 (1996).

[Kallberg 2015] Kallberg, J.: 'A right to cybercounter strikes: The risks of legalizing hack backs'; IT Professional, Vol. 17, No. 1 (2015), pp. 30–35. https://doi.org/10.1109/MITP.2015.1

[Kerstens and Veenstra 2015] Kerstens, J., Veenstra, S.: 'Cyber Bullying in the Netherlands: A Criminological Perspective'; International Journal of Cyber Criminology, Vol. 9, No. December (2015), pp. 144–161. https://doi.org/10.5281/zenodo.55055

[Lewis 2006] Lewis, T. G.: 'Critical infrastructure protection in homeland security: defending a networked nation'; Hoboken: Wiley-Interscience (2006).

[Lin 2016] Lin, P.: 'Ethics of Hacking Back: Six arguments from armed conflict to zombies'; (2016).

[Lorenčič 2003] Lorenčič, M.: 'Na šolah se varnostnikov ne branijo'; (2003).

[Loyens 2009] Loyens, K.: 'Occupational culture in policing reviewed A comparison of values in the public and private police'; International Journal of Public Management, Vol. 32, No. 6 (2009), pp. 461–490.

[Lukman and Bernik 2008] Lukman, M., Bernik, I.: 'Ogrožanja kritične infrastrukture iz kibernetskega prostora'; In Varstvoslovje med teorijo in prakso. Ljubljana: Faculty of Criminal Justice and Security (2008), pp. 1–11.

[Malby et al. 2013] Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., Ignatuschtschenko, E.: 'Comprehensive Study on Cybercrime'; New York (2013).

[McGraw 2013] McGraw, G.: '"Active defense" is irresponsible'; (2013).

[Messerschmidt 2013] Messerschmidt, J.: 'Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm'; Columbia Journal of Transnational Law, Vol. 52, No. 1 (2013), pp. 275–324.

[Mihelič, Bernik, Markelj and Zgaga 2017] Mihelič, A., Bernik, I., Markelj, B., Zgaga, S.: 'Investigating the darknet: limitations in Slovenian legal system'; In Proceedings of the 12th International Conference on Availability, Reliability and Security. Reggio Calabria: ACM New York (2017).

[Mihelič and Vrhovec 2017] Mihelič, A., Vrhovec, S.: 'Explaining the employment of information security measures by individuals in organizations: The self-protection model'; In I. Bernik, B. Markelj & S. Vrhovec (Eds.), Advances in cybersecurity 2017. Maribor, Slovenia: University of Maribor Press (2017), pp. 23–34. https://doi.org/10.18690/978-961-286-114-8.2

[Miller and Rowe 2012] Miller, B., Rowe, D.: 'A survey SCADA of and critical infrastructure incidents'; Proceedings of the 1st Annual Conference on Research in Information Technology - RIIT '12, , No. March (2012), p. 51. https://doi.org/10.1145/2380790.2380805

[Miraglia and Casenove 2016] Miraglia, A., Casenove, M.: 'Fight fire with fire: The ultimate active defence'; Information and Computer Security, Vol. 24, No. 3 (2016), pp. 288–296. https://doi.org/10.1108/ICS-01-2015-0004

[Mpoke Bigg 2017] Mpoke Bigg, M.: 'Germany may need constitutional change to allow it to strike back at hackers'; (2017).

[Nurmi and Niemelä 2017] Nurmi, J., Niemelä, M. S.: 'Tor De-anonymisation Techniques'; In Network and System Security (NSS 2017) (2017), pp. 657–671. https://doi.org/10.1007/978-3-319-64701-2_52

[Patrascu and Simion 2014] Patrascu, A., Simion, E.: 'Cyber Security Evaluation of Critical Infrastructures Systems'; In N. Bizon, L. Dascalescu & N. M. Tadatabei (Eds.), Autonomous Vehicles: Intelligent Transport Systems and Smart Technologies. Nova Science Publishers (2014), pp. 185–205.

[Pool and Custers 2017] Pool, R. L. D., Custers, B. H. M.: 'The Police Hack Back: Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime'; European Journal of Crime, Criminal Law and Criminal Justice, Vol. 25, No. 2 (2017), pp. 123–144.

[Prezelj et al. 2008] Prezelj, I., Kopač, E., Svete, U., Grošelj, K., Sotlar, A., Lipicer Kustec, S., Žiberna, A.: 'Definicija in Zaščita Kritične Infrastrukture Republike Slovenije'; (2008).

[Singh and Kempa 2007] Singh, A. M., Kempa, M.: 'Reflections on the study of private policing cultures: key questions, challenges and early leads'; In Police occupational culture: new debates and directions. Oxford: Elsevier Science (2007), p. 297--320.

[Sotlar and Čas 2011] Sotlar, A., Čas, T.: 'Analiza dosedanjega razvoja zasebnega varovanja v Sloveniji - med prakso , teorijo in empirijo'; Revija Za Kriminalistiko in Kriminologijo, Vol. 62, No. 3 (2011), pp. 227–241.

['State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks' 2017] (2017).

[Šturm 2002] Šturm, L.: '34. člen'; In L. Šturm (Ed.), Komentar Ustave Republike Slovenije (2002), pp. 362–367.

[van Dijk, Tseloni and Farrel 2012] van Dijk, J., Tseloni, A., Farrel, G.: 'The International Crime Drop: New Directions in Research'; Palgrave Macmillan (2012).

[Wakefield 2008] Wakefield, A.: 'Private Policing: A View From The Mall'; Public Administration, Vol. 86, No. 3 (2008), pp. 659–678. https://doi.org/10.1111/j.1467-9299.2008.00750.x

[Wendzel and Kasem-Madani 2016] Wendzel, S., Kasem-Madani, S.: 'IoT Security: The Improvement-Decelerating "Cycle of Blame"'; Germany (2016).

[Yar 2005] Yar, M.: 'The Novelty of "Cybercrime": An Assessment in Light of Routine Activity Theory'; European Journal of Criminology, Vol. 2, No. 4 (2005), pp. 407–427. https://doi.org/10.1177/147737080556056

[*Zakon o zasebnem varovanju (ZZasV-1)* 2011] (2011).

[Završnik 2013] Završnik, A.: 'Spletno in mobilno nadlegovanje: pojem, oblike, posledice in soočanje s kazenskim pravom 1.'; Zbornik Znanstvenih Razprav, Vol. 73 (2013), pp. 219–252.

[Zgaga 2011] Zgaga, S.: 'Skrajna sila v mednarodnem kazenskem pravu'; University of Ljubljana (2011).