Fichtner, Laura

Article

What kind of cyber security? Theorising cyber security and mapping approaches

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Fichtner, Laura (2018) : What kind of cyber security? Theorising cyber security and mapping approaches, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 7, Iss. 2, pp. 1-19, https://doi.org/10.14763/2018.2.788

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 7 | Issue 2

What kind of cyber security? Theorising cyber security and mapping approaches

Laura Fichtner
Department of Informatics, University of Hamburg, Germany, fichtner@informatik.uni-hamburg.de

Published on 15 May 2018 | DOI: 10.14763/2018.2.788

Abstract: Building on conceptual work on security and cyber security, the paper explores how different approaches to cyber security are constructed. It outlines structural components and presents four common approaches. Each of them suggests a different role for the actors involved and is motivated and justified by different values such as privacy, economic order and national security. When a cyber security policy or initiative is chosen by policymakers, the analysis of the underlying approach enhances our understanding of how this shapes relationships between actors and of the values prioritised, promoted and inscribed into the concerned technologies.

Keywords: Cyber security, Securitisation, Internet governance, Ethics, Values, Computer Ethics

Article information

Received: 18 Dec 2017 **Reviewed:** 19 Mar 2018 **Published:** 15 May 2018

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/what-kind-cyber-security-theorising-cyber-security-and-mapping-approaches

Citation: Fichtner, L. (2018). What kind of cyber security? Theorising cyber security and mapping approaches. *Internet Policy Review*, *7*(2). DOI: 10.14763/2018.2.788

This paper is part of Networked publics, a special issue of Internet Policy Review *guest-edited by William H. Dutton.*

INTRODUCTION

Cyber security has become a matter of increasing public prominence. This is evidenced by incidents broadly discussed in the media, such as Snowden's 2013 leaks of secret and classified NSA surveillance programmes (Szoldra, 2016), the alleged Russian hacking of the 2016 US national elections (CNN Library, 2018), 2017's Equifax breach, where hackers gained access to sensitive, credit-relevant data on more than 100 million customers (Wattles & Larson, 2017), and the same years' Wannacry attack which held thousands of Microsoft-run computers ransom (Fox-Brewster, 2017). However, the question of what cyber security is about and which kinds of

actions cyber security concerns should lead to remains open. All of the above examples relate to cyber security, yet they are about different issues and concerns, relating to, for example, governmental surveillance, economics of privacy, and cyber security and political decision-making. They also describe different kinds of incidents and breaches, involve different actors, ranging from corporations to intelligence agencies, citizens, and nation states, and focus on different relationships between them.

Common definitions of cyber security often unite or sit above issues, threats, activities and aspects. A German cyber security strategy for example states: "the availability of cyberspace and the integrity, authenticity and confidentiality of data in cyberspace have become vital questions of the 21st century. Ensuring cyber security has thus turned into a central challenge for the state, business and society both at national and international levels" (European Network and Information Security Agency, 2012, p. 4). In 2011, the Dutch Ministry of Security and Justice defined cyber security as a state of "being free from danger or harm caused by the malfunction or failure of ICT or its misuse" (Van Den Berg et al., 2014, p. 4). Others define cyber security as the "harmonisation of capabilities in people, processes, and technologies; to secure and control both authorised and/or unlawful access, disruption, or destruction of electronic computing systems (hardware, software, and networks), the data and information they hold", or as the "effective cyber-secure operations that guarantee pre-set system objectives" (Ani, He, & Tiwari, 2016, p. 170).

This paper explores how such meanings of cyber security arise by identifying four structural components which approaches to cyber security include, and by examining four common approaches to cyber security. The analysis starts with the theoretical framework of Securitisation Studies and David Baldwin's conceptual work on security (Baldwin, 1997; Buzan, Wæver, & de Wilde, 1998; Emmers, 2016). These works have provided answers to the questions of what exactly security is, how security issues are constructed and with what effects these issues are communicated. The two frameworks will be used in a complementary fashion in this paper, in order to build a constructivist account of cyber security. The following section then discusses how the insights this literature provides apply to cyber security in the context of internet governance. The section presents research from science and technology studies (STS) and computer ethics, which have sought to demonstrate the applicability of the Securitisation framework to information technologies and cyber security (Dunn Cavelty, 2013; Hansen & Nissenbaum, 2009; Nissenbaum, 2005; Wolff, 2016). Based on these conceptual clarifications, the paper describes the four structural components identified and proceeds to present and discuss four common approaches to cyber security: as data protection, as safeguarding financial interests, as the protection of public and political infrastructures, and as the control of information and communication flows.

The approaches each differently define the structural components presented, such as the threats they concern (i.e., posed by corporations, hackers, citizens, other states), the objects they protect (i.e., public infrastructures, personal information, economic rules), the cyber security measures they utilise (i.e., technical measures, policies), and the responsibilities they give to actors and stakeholders (i.e., corporate or governmental actors, citizens and individuals). Thus, each approach constructs a unique set of relationships between the actors involved. When actions are taken based on the approach chosen, these relationships are encoded into the technologies concerned. Interestingly, each approach is motivated and justified by its own set of values. This implies that, depending on the underlying approach, actions taken in the name of cyber security can promote the particular values that motivate and justify them. Conversely, cyber security approaches might be favoured depending on the values important to those who are making

decisions.

The article postulates a close connection between cyber security governance, stakeholder relations and the promotion of values such as safety, privacy, fairness, free market competition and democracy. As any cyber security approach chosen shapes this connection, taking a closer look at the approaches behind cyber security initiatives or policies enables a better understanding of which values are prioritized and promoted, and of how relationships and responsibilities are constituted between the participating actors in the public sphere. This makes the question of how decisions about cyber security are made a question of public and political interest. The paper closes with a discussion of its findings and reflections on future research.

SECTION 2: SECURITISATION STUDIES AND THE CONCEPT OF SECURITY

SECURITISATION AND THE COPENHAGEN SCHOOL

A prominent approach to studying security known as the Copenhagen School has taken a constructivist approach to answering the question of what security entails. It offers a framework for studying the construction of security issues and its effects. The Copenhagen School proposes to widen the study of security beyond its traditional focus on military affairs and nation state actors to include a variety of threats posed in various sectors. These can be problematised and responded to by actors located on seperate analytical levels (Buzan et al., 1998, pp. 5–10; Emmers, 2016, p. 132).

The Copenhagen School conceptualises security as a way of establishing relations and relationships. Responses to security issues establish relations between the entities and actors involved, for example between human collectives and groups, or between collectives and their environment (Buzan et al., 1998, p. 10). Further, different kinds of security as they pertain to different sectors (economic security, environmental security, social security) are about different *kinds* of relations. For example, "the political sector is about relationships of authority, governing status, and recognition; the economic sector is about relationships of trade, production, and finance; the societal sector is about relationships of collective identity" (Buzan et al., 1998, p. 7).

The school's constructivist approach holds there is no security issue in itself or by virtue of its 'essence' (Buzan et al., 1998, p. 31; Emmers, 2016, p. 135). Issues are constructed and positioned as security issues within (public and political) discourses. Security is a speech act which moves an issue from the realm of normal politics to the realm of security, a move called *securitisation* (Buzan et al., 1998, pp. 23–26). When an issue is *politicised*, it becomes a matter of policy and governance to be debated and addressed by political procedures of decision-making. When an issue is *securitised,* it moves from the realm of standard political procedures to the realm of security and takes precedence over other issues, allowing for the employment of extraordinary measures outside what would normally be deemed acceptable (Buzan et al., 1998, pp. 21–22). Securitising an issue can thus help to justify certain activities, initiatives and policies and override other concerns as well as ethical or societal considerations.

In order for securitisation to be successful, an audience needs to be convinced of the existence of an existential and imminent threat to a cherished referent object (Buzan et al., 1998, pp. 21–24; Emmers, 2016, p. 132). A referent object is an entity seen as existential and fundamental to the

survival of (human) life and the proper functioning of society. This threat and its power to potential catastrophe justifies precedence over other issues and the abrogation or breach of standard procedures and established rules and protocols (Buzan et al., 1998, pp. 24–25). As Buzan, Wæver and de Wilde put it, when an issue is successfully securitised, the very existence of human life and social order seems at stake: "If we do not tackle this problem, everything else will be irrelevant (because we will not be here or will not be free to deal with it in our own way)" (Buzan et al., 1998, p. 24). Securitisation studies "who securitizes [sic], on what issues (threats), for whom (referent objects), why, with what results, and [...] under what conditions" (Buzan et al., 1998, p. 32).

THE CONCEPT OF SECURITY

Responding to the Copenhagen School of Securitisation, David A. Baldwin, in his article on 'the concept of security', criticises the way Securitisation scholars approach security, as it can lead to the view that security is an "essentially contested concept" (Gallie, 1955) "so value-laden that no amount of argument or evidence can ever lead to agreement" (Baldwin, 1997, p. 10). Rather than thinking of security as an essentially contested concept he finds it to be a confused, insufficiently explicated and under-theorised concept which has fallen short of conceptual work (Baldwin, 1997, pp. 8–9, 24). There is something which distinguishes security issues from other issues, he argues, proposing to define security "in terms of two specifications: Security for whom? And security for which values?" (Baldwin, 1997, p. 13). Baldwin extends these two initial questions by formulating the further questions of 'security from what threats?' and 'by what means? (Baldwin, 1997, pp. 15–16). The formulation of the structural components of cyber security in this paper departs from Baldwin's questions, but excludes his further questions of 'how much security', 'at what costs' and 'in what time period', because the paper focuses on the values cyber security approaches promote and the relationships they create.

To summarise: Securitisation's constructivist perspective on security states that nothing is a security issue in and of itself but rather issues are constructed as security issues. Constructing something as a security issue is a discursive move which equips the issue with a sense of urgency and priority and can be used to convince an audience of the need for taking action. However, as David Baldwin has argued, there are a number of structural questions which characterise security issues and distinguish them from others, such as 'security for whom?' and 'security from which threats?'. The following section applies this constructivist approach to security in order to ask what exactly *cyber security* is and in order to analyse how securitisation applies to information technology and the internet.

SECTION 3: CYBER SECURITY AND INTERNET GOVERNANCE

THE FIELD OF INTERNET GOVERNANCE

Cyber security is a central part of internet governance, a field which is concerned with how to operate the internet on a structural and infrastructural level. The field addresses the technological, political and legal norms and rules of how we interact on and through the internet. Viewing internet governance as a multifaceted, "heterogeneous process of ordering without a clear beginning or endpoint" (Hofmann, Katzenbach, & Gollatz, 2016, p. 1412), scholars study diverse practices which have effects on the internet's structure, infrastructure and operation, like institutional decisions and standardisation processes, governmental policies and the practices of service providers (Hofmann et al., 2016; van Eeten & Mueller, 2013). These

practices are carried out by and include a broad range of actors, such as internet service providers (Marsden, 2013), nation states and their institutions (Deibert, 2009), international bodies like the EU (European Union, 2016), technical experts, and corporate and individual internet users (i.e., van Eeten & Mueller, 2013). A model often discussed with regards to internet governance is multistakeholder governance which refers to the "joint management of Internet resources by governments, business and the civil society in their respective roles" (Cruz-Cunha & Portela, 2015, p. 397). Actors in multistakeholder governance can, amongst others, be states, formal intergovernmental organisations, firms, NGOs, civil society groups or individuals. There are different forms of multistakeholder involvement, depending on the actors involved and the relationships between them (DeNardis & Raymond, 2013).

Cyber security as a central area of internet governance similarly involves and relates different actors. According to Laura DeNardis, cyber security concerns "a variety of solutions and problems related to authentication, critical infrastructure protection, encryption, worms, viruses, denial of service attacks, and data interception and modification" (DeNardis, 2010, p. 10). Cyber security issues can be addressed by various internet governance mechanisms, for example by governance institutions which tackle issues via the design of technologies, protocols and policies or aim to secure infrastructures against breaches and attacks. At the same time, cyber security policies can also function as leverage points for effectuating broader structural effects and shaping relationships between actors (Fichtner, Pieters, & Teixeira, 2016). Together with Wolter Pieters and André Teixeira, I have already highlighted elsewhere the political dimension of cyber security and argued that ways of framing cyber security or making cyber security arguments shape how technological infrastructures are implemented and access and control rights are allocated (Fichtner et al., 2016).

SECURITISATION AND INFORMATION TECHNOLOGY

Researchers from the fields of science and technology studies and computer ethics have identified cases in which alternative definitions of cyber security lead to policies with different, sometimes opposite, effects. For instance, in her essay on "where computer security meets national security", Helen Nissenbaum contrasts two notions of security within the context of ICTs, 'computer security' and 'cyber-security'. She explains how the notions imply different technical measures and protocols because they differ in their subjects and objects of threats (Nissenbaum, 2005). (Technical) computer security is concerned with "[a]ttacks that render systems, information, and networks unavailable to users, including for example, denial-of-service attacks and malware such as viruses, worms, etc. that disable systems or parts of them" or which "threaten the integrity of information or of systems and networks by corrupting data, destroying files or disrupting code, etc." (Nissenbaum, 2005, p. 63). "Cyber-security", in Nissenbaum's terms, on the other hand concerns threats "posed by the use of networked computers as a medium or staging ground for antisocial, disruptive, or dangerous organizations and communications [...or t]hreats of attack on critical societal infrastructures, including utilities, banking, government administration, education, healthcare, manufacturing and communications media" (Nissenbaum, 2005, p. 64) where law enforcement and surveillance agencies are called upon. Together with Lene Hansen, Nissenbaum demonstrates that cyber security is a valid subject of investigation under the Securitisation framework which involves multiple discourses with their own unique constellations of referent objects, reaching across geographical and political boundaries (Hansen & Nissenbaum, 2009).

Taking up Securitisation's focus on discourse, Miriam Dunn Cavelty identifies three dominant metaphors in the cyber security discourse: parasitic metaphors (worms, viruses), space metaphors (new frontier, cyberspace) and ecological metaphors (organism, ecosphere) (Dunn

Cavelty, 2013). She demonstrates how these metaphors conceive of cyber security in ways which warrant different socio-technical responses and allocations of responsibility. When cyberspace is seen as a territory under threat of anarchism, cyber security is about physical infrastructures "subjected to the principles of territoriality and sovereignty" where state actors need to establish law and order, "control and borders" (Dunn Cavelty, 2013, p. 118). Ideas about cyberspace as its own, self-regulating organism conceptualise "the role of the state" less as that of a much-needed authority but rather "of a gardener and facilitator" (Dunn Cavelty, 2013, p. 119).

In her study on cyber security conflicts in internet governance forums, Josephine Wolff similarly presents interesting cases of dispute over the meaning and definition of cyber security, where "conflicting notions of security" sparked debates about which rules to implement (Wolff, 2016). She finds definitions of security take place within a network of corporate and political interests. Accounts of what cyber security entails lead to the implementation of different infrastructural protocols and norms which play out to the advantage of some and to the disadvantage of other stakeholders (i.e., corporations, civil society organisations, governments). In order to sustain the cyber security approach they defended, the involved actors drew upon values and value conflicts, such as whether to prioritise protecting consumer safety and trust or the privacy of campaigners and fundraisers. These positions led to respectively corresponding responses such as permitting or prohibiting WHOIS privacy for websites engaged in commercial transactions (Wolff, 2016).

Scholars such as Nissenbaum, Dunn Cavelty and Wolff have found that, similarly to how Securitisation sees security, cyber security is a contested concept which can be constructed to be about different referent objects, threats and responses. The structural effects cyber security responses can have for internet governance depend on how cyber security is understood and realised and on who or what it ought to protect. Especially when security concerns override other concerns, it is important to carefully dissect what is being presented as a security issue and by whom.

SECTION 4: THE STRUCTURAL COMPONENTS OF CYBER SECURITY

Building on Securitisation's understanding of security as being contingent and constructed within discourses, and on Baldwin's conceptual work on security, this section outlines four structural components which together can build an approach to cyber security. The mapping of these components bases on the vocabulary Securitisation Studies provide and the questions Baldwin has formulated.

REFERENT OBJECTS

Baldwin's first question was "security for who" (Baldwin, 1997, p. 13) which corresponds to what the Copenhagen School calls a *referent object* (Buzan et al., 1998, p. 36). This is the entity, object, system, unit or the like which is considered to be under threat or which ought to be protected. Referent objects are "seen to be existentially threatened and [as having] a legitimate claim to survival" (Buzan et al., 1998, p. 36). They can be concrete or abstract concepts like national sovereignty, political order and collective identities, but also human lives, values such as freedom and equality, the environment, cities, countries or technological infrastructures.

SECURITISING ACTORS

Securitising actors on the other hand are the actors who securitise an issue and propose the existence of a security issue and existential security threat. While Securitisation's notion of 'securitising actors' focuses on who securitises an issue within a discourse, i.e., who proposes or promotes a security issue, I expand the notion and utilise it for also describing actors who take over responsibilities and tasks for ensuring cyber security. This adaptation allows me to add a question of *security by whom* in order to look at who takes over responsibilities and attains certain rights. This question is interesting, because the actors who take over responsibility are those who have to invest resources, but also those who can access and process information as well as control infrastructures.

THREATS

Further, a security *threat* needs to be defined and conceptualised, corresponding to Baldwin's question of "security from what threats". Being defined as a threat implies being an unwanted participant in a technical infrastructure or system: an entity or actor deemed *not* to have certain rights to exert control or access data, for instance. When cyber security concerns the protection of personal communications from governmental surveillance, this implies the governmental institutions which engage in surveillance are understood as a threat and are not deemed to have the right to break into systems or devices or to access information.

RESPONSES

Finally, either explicitly or implicitly, the proposition of certain *responses* or actions to be taken as a reaction to a proposed cyber security threat is another part of an approach to cyber security. Cyber security responses can be named or proposed directly, but they can also be implicit in the way the problem is framed. For instance, if cyber security is understood as data protection, the range of possible responses is limited to those which protect sensitive information. Responses can be realised on different infrastructural levels, take different (technological) forms and can be implemented by different means. They can be technical, for instance, when systems are technically secured against hacking attacks or when data is encrypted in order to be protected from unauthorised access. Other solutions can take place on a legal or policy level, such as when laws and agreements are implemented which define how data can be shared (i.e., the EU-US privacy shield) or, for instance, when organisations put password policies into place. Other possibilities are the establishment of best practices or cyber security education, for example when citizens learn about how phishing attacks operate. In practice, cyber security responses will often involve a combination of responses. Nevertheless, the kind of response put into place is shaped by the assumed causes of a security problem, for instance whether the problem is considered as a technical issue or as a regulatory loophole. Similarly, responses and their effects differ depending on who is made responsible for ensuring cyber security, whether, for example, technologists, engineers, lawmakers, politicians or citizens are held to be responsible.

ACTORS

The roles of referent object, securitising actor or security threat can be taken up by a variety of actors or by a combination of them. These actors can be for instance international institutions such as international governance bodies like the EU, military partnerships like NATO, and international internet governance bodies like the Internet Engineering Task Force (IETF) or the Internet Corporation for Assigned Names and Numbers (ICANN). They can also be states, i.e., governments or heads of state, national institutions like ministries, law enforcement, secret services, political parties, research organisations, etc., or they can be non-governmental groups like activist and political groups, institutes or NGOs. In addition, corporate actors such as

companies, production units or internet service providers can be involved in cyber security issues. And finally, there are individual internet users who can be concerned, either as hackers or as vulnerable groups threatened by certain risks. The way in which an approach to cyber security defines these roles creates relationships between those actors, stating who ought to be protected by whom and by what means, who can control infrastructures and access data and who is deemed an unwanted participant in a technological infrastructure.

Next to human and institutional actors, technologies and technological infrastructures can function as referent objects or cyber security threats, or as the locus of cyber security responses. In many cases, technologies and technological infrastructures are related to human and institutional actors and are similarly located on different organisational levels within the internet infrastructure. Single devices belong to individuals and contain their personal data, corporations have their own networks or offer their services via the networks they sustain, states and public institutions run critical and public infrastructures such as health care or public transport – these infrastructures in turn ensure their smooth functioning as is the case with the electricity network. Individual hackers and organised criminal groups can use software to hack into corporate computer systems or employ botnets to break into people's computers. National and international infrastructures can be targeted by hacker groups or governmental hackers, and individuals' computers can be targeted for surveillance by governments and corporations.

The definition of the four components (referent object, securitising actor, threat, security response) distinguish a security issue from another kind of issue. However, each cyber security approach separately defines and interprets these components, distinguishing cyber security approaches and their consequences from each other. In cyber security practice, a similar mapping out and defining of such elements is called threat modelling, which includes describing the security threat that is being protected against as well as how it is expected to operate in order to penetrate a system or reach a protected asset (Shostack, 2014). The mapping of cyber security approaches in this paper goes beyond the technical notion of threat modelling. While threat modelling is mainly concerned with decision trees along which threats can attempt to compromise a system, the approaches here are concerned with mapping out kinds of threats posed to kinds of systems, the values which sustain them and the distributions of responsibility in resolving them.

SECTION 5: FOUR APPROACHES TO CYBER SECURITY

This section outlines four common approaches to cyber security which differ in their referent objects, such as personal data, economic or political order, national infrastructures and public safety, the technological infrastructures they aim to secure, the threats they conceptualise and the actors they make responsible for ensuring security. The four approaches are separated for analytical purposes and in order to demonstrate how, by defining the structural components outlined above, divergent issues can be understood as cyber security issues. In practice, the approaches can also be entangled: for instance, a cyber security initiative can be oriented at protecting infrastructures against hacks that compromise the functionality of this infrastructure, while at the same time protecting (personal) data flowing through this infrastructure. Cyber security approaches can also be opposed to each other – this is where possibly hard choices have to be made. For instance, should cyber security responses protect personal communications against all kinds of intrusions or should they allow governmental or corporate agents to intercept and analyse communications in order to identify potential threats?

CYBER SECURITY AS DATA PROTECTION

Where cyber security is concerned with the protection of sensitive and personal data and communications, or otherwise confidential information to be protected from interception and wiretapping, it is closely related to privacy concerns and data protection. Threats to data protection can be posed by criminal hackers who aim to break into systems in order to attain information. They can also be posed by governments or corporations, where they for instance engage in surveillance of citizens and consumers, respectively. On a smaller scale, spouses and other individual people close to another person's data can also pose a threat. Thus, there is a variety of actors who can act as threats. What unites approaches to cyber security as data protection is their aim to protect information against threats of unlawful or unwarranted access by other parties and against surveillance and wiretapping. Cyber security as data protection can be addressed by technical means such as techniques of encrypted data storing, transmission and end-to-end messaging. But there are also non-technical kinds of responses, such as data protection legislation. Further, where individual users are seen as capable and responsible, educating them about safe data and internet practices and about privacy-friendly technologies can be another cyber security measure taken within this approach. Within corporations or organisations, this approach can also be taken for instance by instituting password policies for employees.

Which kind of solution is applied in any particular case of cyber security as data protection depends on where trust and responsibilities are placed. Where governments, law enforcement and public institutions are not trusted or even seen as potential threats, technical measures that can be independently developed, tested and implemented might appear as the best solution. This is for instance the case where encrypted messaging apps are developed open-source in order to help prevent private communications from being intercepted. Where governmental institutions and their ability to regulate are trusted and corporations are seen as adversarial, legal measures might be chosen. This is the case, for instance, when it comes to regulations such as the EU's General Data Protection Regulation which posits rules of how corporations can handle the data they collect on citizens. Where criminal activities such as identity theft are concerned, law enforcement might be called upon.

Where cyber security ought to protect data in order to ensure privacy, it often seeks to assert the rights of individuals and (vulnerable) groups and to protect them against more powerful agents, or against, for instance, exploitation and manipulation by companies or intrusive or authoritarian governments. This happens where citizens are protected against governmental overreach or where consumer protections are enforced in the form of responsible data policies. However, cyber security as data protection is also concerned in cases where companies aim to protect their confidential information from industrial espionage or where governments aim to protect their employees and institutions. This is where the approach can overlap with the one presented in the next sections.

A case exemplifying the approach of cyber security as data protection was the case of Apple vs. the FBI in 2016 (Krüger, 2016; Spiegel Online, 2016). In this case, the US Federal Bureau of Investigation, a state institution and national law enforcement unit, requested the technology giant Apple to provide them with software that would enable the agency to break into a suspect's phone in order to access the personal information it had stored. Apple declined this request, arguing that providing the state with software able to break its product's privacy protection would compromise the company's customers' privacy and consequently their trust in the company. In this case, Apple 'sided' with citizens and civil rights activists aiming to protect privacy against possibilities of governmental surveillance. Here, the private information of

customers was supposed to be protected from the threat of governmental surveillance, which could also create security loopholes that could be exploited. In this case, the company acted as the securitising actor: it had put strong encryption on its devises, it refused to crack this encryption, and it argued that doing so would compromise cyber security in the sense of data protection.

CYBER SECURITY AS SAFEGUARDING FINANCIAL INTERESTS

Another cyber security approach is aimed at protecting financial assets or securing commercial revenues. In this area, cyber security is perceived to be steered by the market – if information technologies ought to become more, say, privacy-friendly, this development would need to be enforced via consumer choices. Cyber security ensures compliance with the existing economic rules and laws and ought to protect fair competition and market principles; states and governments have to ensure principles by means of regulation and law enforcement. The exact cyber security response proposed by an approach to cyber security as safeguarding economic interests depends on the kinds of economic losses expected and the revenue models considered. Potential threats can be posed by cybercriminals or blackmailers, other companies and competitors, the governments of other states, political groups and activists, amongst others.

Most companies use ICTs to organise business processes, relying on ICT systems and digitally stored business information. Protecting these systems and confidential information against potential intruders and eavesdroppers guarantees economic advantages and ensures what is understood as fair competition. ICT systems are also responsible for the smooth functioning of production and services. Systems that malfunction as a consequence of intrusion, manipulation and shut-down can result in a loss of revenue. Where services relate to critical infrastructures of public transportation or health care, or where sold products can potentially harm consumers (i.e., self-driving cars) (see for example European Network and Information Security Agency, 2013), cyber security incidents could hurt consumers and lead to a loss of trust in the company, if not legal consequences. In addition, companies hold much personal data; some even make their money off personal data. Protecting this data on behalf of their customers is necessary for complying with the law, but also for maintaining customers' trust.

This last aspect is closely related to the Apple vs. FBI case mentioned in the previous section. When looking at this case from another perspective, it could also be used as an example for the approach presented in this section. While an approach to cyber security as data protection would argue that cyber security responses need to protect people's privacy and personal data, an approach to cyber security as safeguarding economic interests would see the FBI's request as a threat to the company and its revenue by compromising its products and alienating its customers. In this case, cyber security is an essential business asset. What is thus important from this perspective are economic and financial aspects and the values related to those.

Another case of cyber security as safeguarding economic interests is the enforcement of (digital) copyrights. The American "Digital Millennium Copyright Act" prohibits the owners of digital devices from tampering with or breaking any digital locks put on the device in order to protect against copyright infringements by users (Doctorow, 2016; Mullin, 2013). These locks seek, for instance, to prevent the recording of streamed videos. Some have argued that the prohibition to tamper with digital locks actually decreases cyber security however, because it does not allow researchers to test the locks' 'actual', read technical, security or to disclose discovered vulnerabilities (Doctorow, 2016). Hence, the locks can end up making devices more vulnerable, jeopardising the security of individuals' devices and their personal information stored on them.

CYBER SECURITY AS THE PROTECTION OF PUBLIC AND POLITICAL INFRASTRUCTURES

Where politicians and public policy officials talk about cyber security, they often speak about the protection of public, sometimes vital, infrastructures such as communication systems, electric grids, hospitals and public transport. Under the use of advanced information technology, more and more public and vital infrastructures are connected to or operate on the internet. A compromise of these infrastructures can slow down a country's development, upset social order or result in injuries and deaths. In addition, political parties or political systems such as e-voting systems can be attacked and manipulated (CNN Library, 2018). This can threaten due political process and national integrity of elections.

Threats are posed by lone hackers and even experimenting teenagers (Computerwoche, 2008), but the most severe threats seem to be politically motivated and come from political and (para)military groups, activists, and (hostile) states and their military and secret services. They aim at destabilising a country and proving military strength, and are often considered military threats and linked to acts of cyber-warfare (i.e., Davis, 2007; Traynor, 2007). Consequently, securitising actors are often military units and international military alliances as well as national law enforcement and intelligence agencies. Where public and political infrastructures are run by private corporations or as public-private partnerships, responsibilities can also be assigned to companies. One example of such an attack on public infrastructure is the virus Stuxnet which seemed to have aimed at slowing down Iran's nuclear developments (Stöcker, 2010). Another example are the attacks on US electricity and water infrastructures, which appear to continue since 2016 and are allegedly carried out by Russian actors (Perlroth & Sanger, 2018).

Within this approach, possible responses can take the form of systems and security engineering which ought to make breaking into and manipulating systems more difficult and provide effective ways for mitigating breaches. Technical measures are network monitoring and data analysis; some even propose more offensive strategies which fight back and attack the attackers themselves (Roggeveen, 2017; Paganini, 2013). Developing cyber security standards and policies (i.e., NIST, 2014) and applying political diplomacy are additional responses.

Of course, this approach can also have overlaps with other approaches, for instance where infrastructures are run by private companies or as public-private partnerships, involving corporate financial interests. What separates this approach from the others is its focus on cyber security as being about protecting public and political infrastructures in order to ensure their smooth functioning within our societies and the kinds of lives they enable for us. The values that motivate such an approach to cyber security are social and public values such as public safety, national integrity, peace and democracy. Protecting public infrastructures is essential for the functioning of society as a whole: it ensures things like the internet, electricity, health care and public transport and protects public safety and the functioning of political structures.

CYBER SECURITY AS CONTROL OF INFORMATION AND COMMUNICATION FLOWS

The final approach to cyber security presented can at times appear antagonistic to the other approaches. It is often more concerned with breaking into systems than with protecting against breaches. What holds together different cyber security issues and responses within this approach is their shared aim of controlling information flows. The approach focuses on the human use of communication systems for a variety of purposes including political activism, activities and opposition, spreading political messages, (false) information and propaganda, or for organising (politically motivated) acts of violence.

Approaches to cyber security as the control of information and communication flows focus on methods which involve extensive data surveillance. There are two separate aspects involved: one is surveillance of communications and collection of intelligence in order to identify potential threats, and the second is utilising surveillance in order to directly moderate and censor information shared online. Both aspects are concerned with the content of online communications and the transition between them is fluid. Surveillance can be used to identify undesired political activism or political violence, but also to regulate what is allowed to be communicated and to enforce censorship rules. The collection and analysis of information flows on the network can be used for identifying and countering potential threats and conspiracies, but also for regulating the content of information and opinions posted and shared.

In many cases, governments, state institutions and regulators act as securitising actors – security issues are often evoked where justifications for governmental surveillance are made (Owen & McCarthy, 2013). But corporations and internet service providers are also involved. They are called upon to combat hate speech and fake news and provide governments, intelligence and law enforcement agencies with data about their users (Eddy & Scott, 2017; MacAskill & Rushe, 2013; Timm, 2014; Wong, 2016). They further apply measures according to their own terms and conditions, following values they see fit and acceptable for the majority of their customers (Bhattacharya, 2016; Heath, 2017). An example is a law passed in Germany in 2017, the so-called *Netzwerkdurchsetzungsgesetz* (or *NetzDG*, for its acronym in German), which obliges social media companies to delete illegal posts which have been flagged or reported by users, such as those perpetrating hate speech, within 24 hours ("Germany starts enforcing hate speech law," 2018).

Approaches to cyber security as the control of information and communication flows are often motivated by values like national security, the rule of law, public safety and political stability. Here, the approach overlaps with approaches to cyber security as the protection of public and political infrastructures. Both can aim at ensuring public safety and political integrity, and technical surveillance and data analysis techniques can be used to identify threats on the network. However, while the former approach is concerned with ensuring the smooth functioning of infrastructures operated *by* ICTs, this approach is concerned with identifying threats via intelligence on human activity and then acting upon those threats, either outside the infrastructure or by controlling communications.

Where surveillance is used for identifying threats via the interception of communications, this is often justified by a need to protect against activities seen to threaten the state, its stability and integrity, and public order. For instance, the government's stance in the Apple vs. FBI case was that breaking into the IPhone would provide important information for ensuring national security. Similarly, where online information and content is censored, this information is often seen as seditious, as threatening social order and societal and political norms and rules.

Whether or not activities of data-based surveillance and online content moderation should be considered cases of cyber security remains contested. One may argue that they are rather activities which use data analytics in order to identify and prevent threats for diverse security purposes, but that in contrast to the other approaches they are not necessarily concerned with securing technical systems. At the same time, identifying and controlling information flows in order ensure predefined system functionality, and in order to control who can do what, seems like a prototypical cyber security activity even though the aim is not to keep threats from breaking into technical systems. Further, many of the activities which are carried out under this approach will require extensive cyber security expertise. Surveillance – collecting and analysing

data streams – is a major activity within the umbrella of cyber security and there is significant overlap and entanglement of issues of information control with cyber security issues. For these reasons, the paper includes this approach to cyber security here. In addition, it would have seemed reductive to bracket out from a conceptual discussion on cyber security the whole range of activities related to surveillance, censorship and online content moderation.

SECTION 6: DISCUSSION AND FUTURE RESEARCH

Building on previous research in STS and computer ethics, the paper presents a constructivist approach to cyber security, describing how issues can be constructed as cyber security issues, sometimes with adverse effects. The framework the paper develops bases on the Copenhagen School of Securitisation, which states issues are securitised within discourses - constructed as security issues where an existential and imminent threat is posed to a cherished, invaluable referent object - in order to justify actions presented as necessary security responses. Combining the insights Securitisation provides with David Baldwin's conceptual work on security, the essay proposed four structural components which build an approach to cyber security. Which approach to cyber security is then chosen or given priority will determine how these structural components are filled and which roles are given to the actors involved, relating them in definite ways.

The paper's distinction between four common approaches to cyber security is of analytical nature. Concrete instances of cyber security located within the four approaches can still vary – for instance, data can be protected against governmental or against corporate surveillance. Approaches to cyber security can have overlaps where threats, referent objects or security responses are identical – from the viewpoint of the companies which operate public infrastructures, the protection of public and political infrastructures for instance can coincide with safeguarding their economic interests. Approaches stand in opposition to each other where the threat of one is the securitising actor of the other, and where the one approach's response jeopardises the other's security, for instance when data protection threatens surveillance mechanisms.

THE ROLE OF VALUES FOR CYBER SECURITY DECISIONS

Each cyber security approach is motivated and justified by appealing to values which it aims to promote, such as freedom of speech, democracy, social order, economic freedoms, public safety and human rights. The set of values underlying an approach to cyber security shapes how the approach defines its structural components. Approaches aiming to protect privacy, freedom of speech, economic interests, human rights, public safety, political order, human integrity, national sovereignty, cultural norms, fair competition, and so on, will differ in the referent objects, technological infrastructures and threats they consider, the actors they trust, and the priorities they have. A debate about which cyber security issues we face and which cyber security responses to adopt is not just a debate about which responses are most effective or in least conflict with other values such as privacy or innovation. Rather, it is a debate about which values ought to be upheld and promoted, which values we, as a society, find most important or see most threatened.

The paper thus demonstrates how deeply intertwined seemingly technical matters of cyber security can be with societal, political and ethical issues. There are close connections and interactions between decisions on internet and cyber security governance, stakeholder relationships and social, ethical and political norms and values. Paying attention to which kind

of approach underpins a debate on cyber security or motivates responses to cyber security issues can help us understand the values at stake and the relationships enforced. Thus, analysing adopted approaches to cyber security can tell us which values might be most important to those making the decisions as well as which kind of audience can potentially be convinced by the approach and the case it makes for why cyber security is important. Similarly, we have elsewhere argued that ways of framing cyber security can be a means of governing information infrastructures and mediating access and control rights (Fichtner et al., 2016).

How values, approaches to cyber security and audiences relate, and how securitisation works in the case of cyber security, are empirical questions, but they also raise normative ones. Questions which follow from a constructivist approach to cyber security are how the term *should* be defined and which responses it should entail. If it is true that presenting an issue as a cyber security issue is a convincing argument for taking action, this is a highly significant aspect for public and political debate. The question then remains of what we *ought* to do and what the ethics are of *talking* about cyber security. How resources for cyber security should be allocated or which approaches to cyber security should be prioritised are other related questions. Another important point is how to critically reflect on the respective approach taken, as there might be overlaps or conflicts with other approaches and the values they safeguard. For instance, a completely anonymous network might protect sensitive information about its participants but endanger network security. When only one approach to cyber security is considered, this might distract from other important issues or obscure that only certain kinds of risks are secured against, while others are not considered.

SCOPE OF THE FRAMEWORK

The paper presented one framework for conceptualising cyber security by distinguishing cyber security approaches based on the structural components presented above and the values which motivate and justify them. This perspective says little about how cyber security issues *should* be approached; the normative claim it makes is that when devising cyber security policies, we *should* pay attention to the approach chosen and make explicit the underlying norms and assumptions. The proposed conceptualisation also says little about how to implement cyber security, about the process of how to *do* cyber security, how to build cyber security capacities or develop cyber security incentives.

Other frameworks for conceptualising cyber security differ in their analytic focus and in the kind of analysis they enable. For instance, the Oxford Cybersecurity Capacity Maturity Model is concerned with cyber security capacity building (Global Cyber Security Capacity Centre, 2014). The model distinguishes five dimensions of cyber security capacity building which are further divided into factors, which are then analysed based on categories classified according to levels of maturity. While the model makes other distinctions than the ones proposed in this paper, it includes references to the distinctions proposed here. For example, it talks about involved actors as “strategy ‘owners’” (Global Cyber Security Capacity Centre, 2014, p. 8), which corresponds to the notion of securitising actors, and it includes reference to kinds of cyber security responses such as legal, technical and educative ones. It also distinguishes between a number of actors and sectors, such as civil society, the public and private sectors and refers to the responsibilities and responses of corporate, governmental and military actors (Global Cyber Security Capacity Centre, 2014, pp. 17 & 28). The model does not systematically differentiate between various threats, but for instance includes a subcategory of “privacy, data protection & other human rights” (Global Cyber Security Capacity Centre, 2014, p. 30), and it discusses the protection of critical infrastructure. Different frameworks for conceptualising cyber security do not necessarily need to compete, but can complement each other.

DIRECTIONS FOR FUTURE RESEARCH

The paper opens up new empirical, conceptual and normative questions for future research. An empirical analysis could aim at measuring the effects of securitisation with regards to cyber security and at refining and expanding the cyber security approaches presented. The challenge here would be to identify the discourses relevant for cyber security decisions. Central empirical questions are: who securitises issues with regard to information technologies, who is the relevant audience to be convinced, and who makes decisions with regards to cyber security? Is there a public or political discourse on these matters, and if yes, for which questions? And which questions are perhaps left to technologists and internet governance forums? While there might be a quite obvious public discourse on questions of privacy and national security, are there other aspects of cyber security not or only very implicitly debated? And in what way, if at all, does cyber security take up a special status that allows for the implementation of special responses? Or does cyber security turn out to be just one issue of many in internet governance? A conceptual question on the other hand would be what counts as cyber security and what does not. So, which activities does the label 'cyber security' describe? Here, conceptual clarifications about how the meaning and usage of the term relates to other security terminology used with regards to information technology, such as information security, digital security and internet security, could help shed further light on conceptual matters of cyber security. These questions are closely intertwined with normative questions, namely what *should* be labelled a cyber security issue and why? Which cyber security approaches should be prioritised and with what effect? Which values should cyber security initiatives promote? Who should make decisions concerning cyber security issues and how should they approach these issues? And which approaches to cyber security might be problematic because they conflict with other approaches and the values they aim to uphold?

ACKNOWLEDGEMENTS

I would like to thank Wolter Pieters, André Teixeira and Jan van den Berg for their supervision, support and feedback during my time at TU Delft. The discussions with them provided an important contribution to developing the ideas presented in this paper. I would also like to thank Michel van Eeten and his cyber security group for inspiring discussions on the issues discussed in this paper. Finally, I would like to thank Judith Simon for valuable feedback on an earlier draft.

REFERENCES

Ani, U. P. D., He, H. M., & Tiwari, A. (2016). Human capability evaluation approach for cyber security in critical industrial infrastructure. In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity* (501st ed., pp. 169–182). Cham, CH: Springer. doi:10.1007/978-3-319-41932-9_14

Baldwin, D. A. (1997). The concept of security. *Review of International Studies*, *23*(1), 5–26. Retrieved from https://www.cambridge.org/core/journals/review-of-international-studies/article/the-concept-of-security/67188B6038200A97C0B0A370FDC9D6B8

Bhattacharya, A. (2016, October 12). Facebook is under fire for censorship again, this time for blocking an image of a mammogram. *Quartz*. Retrieved from https://qz.com/807427/facebook-fb-is-under-fire-for-censorship-again-this-time-for-blocking-an-image-of-a-mammogram/

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder, CO: Lynne Rienner Pub. Retrieved from https://books.google.de/books/about/Security.html?id=j4BGr-Elsp8C&redir_esc=y

CNN Library. (2018, February 21). 2016 presidential campaign hacking fast facts. *CNN*. Retrieved from http://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html

Computerwoche. (2008, January 18). Infrarotes Licht als Steuersystem: Polen: Teenager hackt Straßenbahn mit Fernbedienung. Retrieved from https://www.tecchannel.de/a/polen-teenager-hackt-strassenbahn-mit-fernbedienung,1744101

Cruz-Cunha, M. M., & Portela, I. M. (Eds.). (2015). *Handbook of research on digital crime, cyberspace security, and information assurance*. Hershey, PA: IGI Global.

Davis, J. (2007, August 21). Hackers take down the most wired country in Europe. *Wired*. Retrieved from https://www.wired.com/2007/08/ff-estonia/

Deibert, R. J. (2009). The geopolitics of internet control: Censorship, sovereignty, and cyberspace. In A. Chadwick & P. N. Howard (Eds.), *Routledge Handbook of Internet Politics* (pp. 323–336). Oxon, UK: Routledge.

DeNardis, L. (2010). The emerging field of internet governance. *Yale Information Society Project Working Paper Series*. doi:10.2139/ssrn.1678343

DeNardis, L., & Raymond, M. (2013). *Thinking clearly about multistakeholder internet governance. GigaNet: Global Internet Governance Academic Network, Annual Symposium 2013*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2354377

Doctorow, C. (2016, July 21). America's broken digital copyright law is about to be challenged in court. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/jul/21/digital-millennium-copyright-act-eff-supreme-court

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105–122.

doi:10.1111/misr.12023

Eddy, M., & Scott, M. (2017, June 30). Delete hate speech or pay up, Germany tells social media companies. *New York Times*. Retrieved from https://www.nytimes.com/2017/06/30/business/germany-facebook-google-twitter.html

Emmers, R. (2016). Securitization. In A. Collins (Ed.), *Contemporary Security Studies* (pp. 168–181). Oxford, UK: Oxford University Press.

European Network and Information Security Agency. (2012). *National cyber security strategies: Setting the course for national efforts to strengthen security in cyberspace*.

European Union. European Union General Data Protection Regulation (2016). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

European Union Agency for Network and Information Security. (2013). *Smart grid threat landscape and good practice guide*. doi:10.2824/34387

Fichtner, L., Pieters, W., & Teixeira, A. (2016). Cybersecurity as a Politikum: Implications of security discourses for infrastructures. In *NSPW '16 Proceedings of the 2016 New Security Paradigms Workshop* (pp. 36–48). New York, New York, USA: ACM Press. doi:10.1145/3011883.3011887

Fox-Brewster, T. (2017, May 12). An NSA cyber weapon might be behind a massive global ransomware outbreak. *Forbes*. Retrieved from https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/#5d074224e599

Gallie, W. B. (1955). Essentially Contested Concepts. *Proceedings of the Aristotelian Society*, 56, 167–198.

Germany starts enforcing hate speech law. (2018, January 1). *BBC News*. Retrieved from http://www.bbc.com/news/technology-42510868

Global Cyber Security Capacity Centre. (2014). *Cyber security capability maturity model (CMM)*. Retrieved from http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM Version 1_2_0.pdf

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly*, *53*(4), 1155–1175. doi:10.1111/j.1468-2478.2009.00572.x

Heath, A. (2017, June 28). Facebook's rules on hate speech leaked in new investigation. *Business Insider Deutschland*. Retrieved from http://www.businessinsider.de/facebook-hate-speech-rules-leaked-2017-6?r=US&IR=T

Hofmann, J., Katzenbach, C., & Gollatz, K. (2016). Between coordination and regulation: Finding the governance in Internet governance. *New Media & Society*, *19*(9), 1406–1423. doi:10.1177/1461444816639975

Krüger, P. S. (2016, March 17). Warum der Streit zwischen Apple und dem FBI so wichtig ist. *Süddeutsche Zeitung*. Retrieved from http://www.sueddeutsche.de/digital/verschluesseltes-iphone-warum-der-streit-zwischen-apple

-und-dem-fbi-so-wichtig-ist-1.2908166

MacAskill, E., & Rushe, D. (2013, November 1). Snowden document reveals key role of companies in NSA data collection. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/nov/01/nsa-data-collection-tech-firms

Marsden, C. T. (2013). Network neutrality: A research guide. In I. Brown (Ed.), *Research Handbook on Governance of the Internet* (pp. 419–444). Cheltenham, UK: Edward Elgar Publishing.

Mullin, J. (2013, March 6). Copyright reformers launch attack on DMCA's "digital locks" rule. *Ars Technica*. Retrieved from https://arstechnica.com/tech-policy/2013/03/copyright-reformers-launch-attack-on-dmcas-digital-locks-rule/

National Institute of Standards and Technology. (2014). *Framework for improving critical infrastructure cybersecurity*.

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology*, *7*(2), 61–73. doi:10.1007/s10676-005-4582-3

Owen, P., & McCarthy, T. (2013, October 29). Intelligence officials defend surveillance tactics in Congressional hearing. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/oct/29/nsa-files-us-intelligence-officials-testify-in-congress-live-coverage

Paganini, P. (2013, July 18). The offensive approach to cyber security in government and private industry. *Infosec Institute*. Retrieved from http://resources.infosecinstitute.com/the-offensive-approach-to-cyber-security-in-government-and-private-industry/#gref

Perlroth, N., & Sanger, D. E. (2018, March 15). Cyberattacks put Russian fingers on the switch at power plants, U.S. says. *The New York Times*. Retrieved from https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html

Roggeveen, B. (2017, August 8). NATO needs an offensive cybersecurity policy. *Atlantic Council*. Retrieved from http://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-an-offensive-cybersecurity-policy

Shostack, A. (2014). *Threat modeling: Designing for security*. Indianapolis, IN: John Wiley & Sons. Retrieved from https://news.asis.io/sites/default/files/Threat Modeling.pdf

Spiegel Online. (2016, March 2). Apple vs. FBI: Jetzt geht es auch offiziell um mehr als ein iPhone - SPIEGEL ONLINE. Retrieved from http://www.spiegel.de/netzwelt/netzpolitik/apple-vs-fbi-nur-ein-iphone-jetzt-geht-es-auch-offiziell-um-mehr-a-1080209.html

Stöcker, C. (2010, December 26). Angriff auf Irans Atomprogramm: Stuxnet-Virus könnte tausend Uran-Zentrifugen zerstört haben. *Spiegel Online*. Retrieved from http://www.spiegel.de/netzwelt/netzpolitik/angriff-auf-irans-atomprogramm-stuxnet-virus-koennte-tausend-uran-zentrifugen-zerstoert-haben-a-736604.html

Szoldra, P. (2016, September 16). This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks. *Business Insider*. Retrieved from http://www.businessinsider.de/snowden-leaks-timeline-2016-9?r=US&IR=T

Timm, T. (2014, October 17). The government wants tech companies to give them a backdoor to your electronic life. *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2014/oct/17/government-internet-backdoor-surveillance-fbi

Traynor, I. (2007, May 17). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*. Retrieved from https://www.theguardian.com/world/2007/may/17/topstories3.russia

Van Den Berg, J., Van Zoggel, J., Snels, M., Van Leeuwen, M., Boeke, S., Van De Koppen, L., … De Bos, T. (2014). On (the emergence of) cyber security science and its challenges for cyber security education. *Proceedings of the NATO IST-122 Cyber Security Science and Engineering Symposium*, 1–12. Retrieved from https://www.csacademy.nl/images/MP-IST-122-12-paper-published.pdf

Van Eeten, M. J. G., & Mueller, M. (2013). Where is the governance in Internet governance? *New Media & Society*, *15*(5), 1–17. doi:10.1177/1461444812462850

Wattles, J., & Larson, S. (2017, September 16). How the Equifax data breach happened: What we know now. *CNN Tech*. Retrieved from http://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html

Wolff, J. (2016). What we talk about when we talk about cybersecurity: Security in internet governance debates. *Internet Policy Review*, *5*(3). doi:10.14763/2016.3.430

Wong, J. I. (2016, February 19). Here's how often Apple, Google, and others handed over data when the US government asked for it. *Quartz*. Retrieved from https://qz.com/620423/heres-how-often-apple-google-and-others-handed-over-data-when-the-us-government-asked-for-it/