International Journal of Cyber Warfare and Terrorism
Volume 6 • Issue 2 • April-June 2016

Reconceptualising Cyber Security:
Safeguarding Human Rights in the Era of Cyber Surveillance

Andrew N. Liaropoulos, University of Piraeus, Piraeus, Greece

ABSTRACT

The cyber security discourse is dominated by states and corporations that focus on the protection of critical information infrastructure and databases. The priority is the security of information systems and networks, rather than the protection of connected users. The dominance of war metaphors in the cyber security debates has produced a security dilemma, which is not sufficiently addressing the needs of people. This article underlines this shortcoming and views cyber security through a human-centric perspective. Freedom of expression and the right to privacy are under attack in the era of cyber surveillance. From a human-centric perspective such rights should be understood as a critical part of cyber security. Human rights protections need to be effectively addressed in the digital sphere and gain their place in the cyber security agendas.

KEYWORDS

Big Data, Cyber Security, Freedom of Expression, Human Rights, National Security, Privacy, Surveillance

INTRODUCTION

Over the past two decades, the evolution of cyberspace has impacted almost every aspect of human life. The increase in the speed, volume, and range of communications that cyberspace offers has transformed the way societies interact, how companies deliver services, and how people are governed. The Internet of Things (IOT) and Big Data are already affecting a wide range of social activities (Cukier & Mayer-Schoenberger, 2013). The cyber domain also poses a growing number of challenges to security. Critical national infrastructures are vulnerable to cyber attacks, and the global economy is exposed to the threats of cyber-espionage and cybercrime. Worms, viruses, sophisticated Distributed Denial of Service (DDoS) attacks, and spam cost the global economy billions of dollars. Cases such as the cyber attacks on the online banking system in Estonia and the use of the Stuxnet worm to harm Iran's nuclear program demonstrate the crucial role of cyberspace for national security. Naturally, states have defined cyberspace in their military and security doctrines as a new domain of conflict.

The cyber security discourse is predominantly shaped by the notion of national security. The release of national security policies and governmental reports, the establishment of cyber-commands and Computer Emergency Response Teams (CERTS), the amount of money spent to defend cyberspace, and the discussion of a cyber-arms race are indicative of this trend (Kramer, Starr, & Wentz, 2009). Although this approach is to a large extent justified, it is also deficient, since it does not consider the human rights protections of around 2.7 billion Internet users (Mihr, 2014, p. 26). Over the past years, the development of Internet censorship techniques and Edward Snowden's revelations about the global surveillance carried out by the United States National Security Agency (NSA) vividly demonstrate that Internet freedom, anonymity, and personal data are constantly

DOI: 10.4018/IJCWT.2016040103

under attack. Citizen's communications are vulnerable to interception and surveillance (Comninos & Seneque, 2014). Therefore, cyber security should not only address the security threats against the state and the private sector, but also (if not primarily) the needs of people.

This article shifts the focus of cyber security from the protection of critical national information infrastructures to that of human rights in cyberspace. The goal is to point out the need for a human-centric approach that addresses digital human rights violations, Internet freedom, and privacy of data. The first section of the article briefly reviews the concept of cyber security and analyses the prevailing approach that perceives cyber security as a national security issue. What is the meaning of the term 'cyber security' and what is it in cyberspace that needs to be protected? The paradoxes of the cyber security dilemma reveal the misperceptions regarding the nature of threats in cyberspace and the referent object of security. The second section reviews examples of human rights violations in cyberspace. Cyber surveillance, internet filtering tools and online censorship are some of the measures used by states. The final section addresses the need for an alternative view of cyber security, one in which the human element is at the epicentre. The argument is that people should have their human rights protected, both offline and online. The unwillingness of states to endorse these rights and the lack of a global governance regime, sketch a rather gloomy picture for the future of human rights in cyberspace.

DECONSTRUCTING CYBER SECURITY

Cyberspace has become an integrated part of human society, and society's dependency upon its infrastructure is constantly increasing. When approaching a contested concept such as cyber security, the reader has to bear in mind the following. First of all, there is no explicit definition of what constitutes cyber security, partially because a universally accepted definition of cyberspace is still lacking. Cyberspace is a term whose definition is hard to pin down and is widely used as a synonym for Internet or the World Wide Web (Betz & Stevens, 2011, p. 13). A popular definition is that of Daniel Kuehl, who defines cyberspace as "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies" (Kramer, Starr, & Wentz 2009, p. 28). The critical question when approaching cyber security is whether one views cyberspace as a global network that involves solely hardware, software, and information systems, or also people and the wide range of social interactions that takes place within this network.

The second issue is that there is a plethora of terms that describe aspects of cyber security. Information security, ICT security, network security, Internet security, and critical information infrastructure protection are some of the terms that are commonly used by scholars and state officials (Klimburg, 2012, pp. 8-13). This terminology covers different types and levels of risk in cyberspace, raising legitimate concerns about the referent object of cyber security (Kovacs & Hawtin, 2013). Adding to the conceptual confusion is the fact that all the above terms, acquire various interpretations when they are placed within a political context. The interpretations regarding the exercise of state sovereignty in cyberspace, the approaches to solving the attribution problem, the ways of establishing cyber deterrence and the thin lines between information security and internet censorship vary in each state (Klimburg, 2012, pp. 20-28; Nocetti, 2015). Since states have different national agendas and different capabilities in cyberspace, they will also have different priorities when addressing the security needs of government, industry, and citizens in the cyber domain (Hare, 2010; Ventre, 2012). Depending on the case, national security priorities in cyberspace may not only involve the

confrontation of hackers, criminals, terrorists, or other states, but also the control or even manipulation of information flow and data.

The last and often a neglected issue, has to do with the fact that security was not a main concern in the early phases of cyberspace development. The logic of its architecture was flexibility and openness and not security and reliability. In the initial design of APRANET and the relevant information infrastructure that followed, the priority was to create an open system, where researchers could share ideas by bypassing the constraints of time and distance. The promise of the Internet was to serve as a domain where individuals could interact, follow news, and share information and ideas freely (Brantly, 2014, p. 133, 150).

The goal of any national security policy is to provide its citizens a secure environment. Taking for granted that modern societies depend on the functioning of ICTs, it only makes sense to assume that a purpose of any national cyber security policy would be to provide its citizens a secure cyber environment. In policy terms, this purpose translates into protection of critical national infrastructures. States are, therefore, developing offensive and defensive cyber-weapons in order to secure their assets in the cyber domain (Brantly, 2014). In the relevant security and military doctrines, references to offense-defence theory, deterrence theory, centre of gravity, arms race, and doom scenarios abound. By emphasizing the strategic and military aspects of cyberspace and not the socio-political ones, states perceive cyber security as a zero-sum game (Dunn Cavelty, 2012).

In their efforts to secure cyberspace, states are trapped in the classic security dilemma (Jervis, 1978). This security dilemma arises from the situation of anarchy that exists in the international system. By striving to increase their states' security—usually by enhancing their military capabilities—states unconsciously make other states feel less secure. The result is a perpetual spiral of security-insecurity. This dilemma can be broken down into a two-level strategic game. At the first level, the dilemma of interpretation results from the uncertainty about the motives, intentions, and capabilities of other actors. At the second level, decision makers need to determine how to react. The dilemma of response only begins when the dilemma of interpretation has been settled (Booth & Wheeler, 2008).

As in the real world, uncertainty and mistrust are also present in cyberspace. States feel insecure about the motives and cyber capabilities of other actors and, therefore, develop offensive and defensive cyber-weapons. Since there is nothing to prevent states from trespassing the digital borders of other states, more insecurity is created (Brantly, 2014, p. 133). This spiral of insecurity produces the dilemma of interpretation and the dilemma of response. At both levels, the current approach to cyber security focuses on the protection of critical national infrastructures (public and private) and not on the rights of citizens. At the interpretation level, cyber attacks against information infrastructures as well as worms and viruses are perceived as cyber threats and not violations of privacy and/or freedom of speech (Dunn Cavelty, 2014, p. 704). The 'human' element as an object of security is not only deemphasized, but it is also considered as part of the threat spectrum (hackers, for instance). Any individual with a computer connected to the Internet and the necessary technical skills constitutes a potential national (cyber) threat (Lucas, 2015). Likewise, at the response level, the goal is the protection of the critical national infrastructures and not the ability of people to gain access to the resources of cyberspace and to use those resources according to their needs and preferences.

The cyber security dilemma not only creates a spiral of insecurity at the international level between states, but it has also negative implications within the states. The cyber capabilities that are developed in order to defend and secure states' critical national infrastructures are also used against their own people. Citizens are trapped in the 'liberty versus security' dilemma, where they have to give up their civil liberties in order to be more secure (Mordini, 2014, p. 625). In other words, cyber security is used as a pretext for governments to sensor, control and target online content. For example, the argument behind the Cyber Intelligence Sharing and Protection Act (CISPA) was to empower the US government and corporations to protect the national information infrastructure from foreign cyber attacks. CISPA enables companies to pass sensitive user data to the government without a warrant (Kovacs & Hawtin, 2013, p. 1). Private companies collect a vast amount of personal data (customers'

preferences) and governments are only a click away from these private databanks (Etzioni, 2015, p. ix). Another example is the use of encryption to protect our private details, during communications. Banning encrypted messages could be perceived as a violation of both the right to privacy and online anonymity; but at the same time, it could be justified for reasons of national security (Green & Rossini, 2015, p. 8). Technology and thereby encryption is neither good nor bad. The same encryption that protects governments and corporations is also used by citizens and terrorists.

In such cases, citizens are not considered the beneficiaries, but rather the victims of national cyber security policies (Brantly, 2014). The side effect of the cyber arms race is a reduction in Internet freedom within states. Filtering technologies that limit access to certain sites, restrictions on the use of encryption, development of Internet kill switches and of surveillance mechanisms to monitor online activities are techniques that have a profound effect on privacy, anonymity, and thereby security (Brantly, 2014, p. 142). The counter-censorship techniques that were used during the 'Arab Spring' (Deibert, 2015) and the Snowden revelations about the global surveillance carried out by the NSA in the name of counterterrorism (Bajaj, 2014) are vivid examples of the dark side of cyberspace.

HUMAN RIGHTS VIOLATIONS IN CYBERSPACE

Individuals around the world are constantly at risk of human rights violations related to cyberspace. Governments employ a variety of measures that violate freedom of expression and the right to privacy, like targeting dissident voices, internet filtering practises or even disconnecting access to ICTs. Below are some examples of cyber surveillance and online censorship.

In 2009, the re-election in Iran of President Mahmoud Ahmadinejad led to a social uprising of young Iranians, claiming that the votes were manipulated and calling for an investigation on the voting fraud. Iranians used social media, mainly Twitter to disseminate information about the protests. During the social uprising in Iran, social networking sites were blocked by the regime and the intelligence and security services managed to identify and close down the activities of those promoting dissent (Liaropoulos, 2013, p. 8). In Tunisia, the self-immolation of the 26-year-old fruit and vegetable seller Mohamed Bouazizi on 17 December 2010, triggered nationwide protests against the oppressive government of Ben Ali. The regime responded by disrupting the flow of information in social media, by hacking e-mail and Facebook accounts. Likewise in Egypt, the protesters demanded Mubarak's resignation and the reinstitution of democracy. The protesters used social media not only to spread the message, but also to share content like online maps and encryption techniques. The regime soon realized the importance of social media for its political survival and intensified the online censorship. The Egyptian police monitored social networks, email accounts of dissidents as well as Skype and arrested dissidents that were responsible for coordinating the protests. In late January 2011, the regime, in a desperate move to control the information flow, decided to cut off access to Internet for a few days (Liaropoulos, 2013, p.9). In January 2010, Google announced that a computer attack originating from China had penetrated its corporate infrastructure and stolen information from its computers, most likely source code. The attacks also targeted Gmail accounts of some human rights activists and infiltrated the networks of 33 companies (Thomas, 2010).

A recent study by the European Parliament titled 'Surveillance and censorship: The impact of technologies on human rights' mentions a variety of measures that states use in order to control the information flow. One such measure that aims to discourage citizens from creating their own blogs and expressing their opinions, is the mandatory registration of online media with pubic authority. In Saudi Arabia, only citizens that can produce 'documents testifying to good conduct' and with a high school diploma are allowed to start their own blog or website. Likewise in Belarus, websites must register using the national domain and be hosted on national territory (2015, p. 10). Another option is the control of the telecommunications industry by governments. China has developed a set of technical solutions like the Great Firewall to block online content from foreign servers. Pakistan is blocking thousands of websites as part of its policies against terrorism, blasphemy and pornography

(2015, p. 10). In Turkey, Google and Facebook were asked to remove political content during the Gezi park protests in 2013 and Twitter and YouTube were blocked before the elections in March 2014 (Epstein, 2013; Tavmen, 2014).

The Snowden revelations about the mass surveillance programs conducted by the 'Five Eyes' (USA, UK, Canada, Australia and New Zealand) demonstrated the magnitude of human rights violations in the digital sphere and the rise of the surveillance state (Greenwald, 2014). In particular, the PRISM program enabled NSA to have direct access to the servers of Apple, Facebook, Google, Microsoft, Skype, Yahoo, Twitter and YouTube (Lyon, 2014, p. 2). The working relationship between intelligence and security agencies on the one hand and private sector one the other hand, raises a number of ethical and legal questions regarding electronic surveillance, citizen privacy and national security (Cropf & Bagwell, 2016). The Snowden disclosures also accentuated the role of Big Data. The capabilities that Big Data practices offer, are transforming the way surveillance is conducted. Personal data are not collected for limited and transparent purposes, whether that is public safety or national security. Big Data reverses the standard policing and intelligence practices, where targets are identified and then data collections follow. Instead, data is now being collected, before deciding on the full range of their actual and potential use. The rationale is that Big Data algorithms will allow us to predict behaviors and events (Lyon, 2014, p. 4). The preemptive logic that Big Data analysis might offer, is challenging the existing legal systems that are based on an after the fact system of penalties or punishments (Lyon, 2014, p. 5).

A HUMAN-CENTRIC PERSPECTIVE ON CYBER SECURITY

Based on the above analysis, the argument can be made that current cyber security policies do not ensure a secure cyberspace for its users. A glimpse at the news and governmental reports proves that cyberspace is not a safe place (Deibert, 2013a; Lucas, 2015). In sharp contrast with the hopes of the early days, the Internet is becoming a tool of authoritarian control. The so-called cyber-utopians failed to predict in the 1990s how useful the Internet would be for propaganda purposes, how states (democratic and authoritarian) would utilize cyberspace for surveillance, and how sophisticated censorship would become. The belief that technology (and thereby ICT) empowers people, rather than state-oppressors is baseless (Morozov, 2011, pp. xiii-xiv). Maintaining privacy on the Internet seems impossible. Governments and corporations are massively collecting private data. Search engines and online social networking sites such as Google and Facebook have detailed profiles of their users, and cell phone companies use GPS technology to track and locate their users. All private data is stored, and people's online behaviour and consumer habits are correlated and passed from companies to governments, most of the time without the knowledge and consent of the users (Kovacs & Hawtin, 2013; Morozov, 2011, p. 163). The transparency reports of Google, Microsoft and Twitter show that most of the requests to companies for user data originate from liberal democracies (Deibert, 2013b, p. 6). Companies that produce social network mining, cell phone tracking, and computer exploitation software are signing contracts with both democracies and authoritarian regimes worldwide. As with the military-industrial complex in the past, the cyber security industry is amplifying the arms race in cyberspace and thereby empowering the cyber surveillance state (Deibert, 2012, pp. 270-271).

A question that is inevitably raised is whether an alternative approach towards cyber security would allow us to escape the cyber security dilemma and ensure the protection of human rights. Would an anthropocentric approach be useful in addressing the need of humans in the cyber realm (Dunn Cavelty, 2014)? Safeguarding human needs in any domain, including cyberspace, raises once more the question about the meaning of security. The term 'security' is usually associated with the absence of threats to scarce values which might threaten the survival of the referent object (Williams, 2008, p. 5).

Security can be approached in a positive and in a negative way. In the latter, security is perceived as the absence of threats to core human values; whereas in the positive sense, it is perceived as the policies and practices that safeguard and empower people to exercise their rights freely and securely.

It is this positive conception of security that seems to be undervalued in the current cyber security discourse. States have historically viewed security in negative terms; and, thus, they also view cyber security as mainly the absence of harm. According to Kovacs and Hawtin, "Cyber security policies should not merely play a defensive role, but a facilitating role, by effectively putting the empowerment and well-being of people at their center. What we are aiming for is for people to be able to be fearless, as long as they are respecting other people's human rights." (2013, p. 7). Human rights refer to those rights guaranteed under the United Nations' Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), and include freedom of expression, freedom of speech, freedom of opinion, and the right to privacy. It is important to note that in July 2012 the UN Human Rights Council confirmed that the same rights that people have offline must also be protected online (Green & Rossini, 2015, p. 8).

So how can states strike a balance between the protection of critical information infrastructure and data flows on the one hand and the right to privacy and online anonymity on the other? And who will be responsible for protecting, implementing and enforcing human rights in cyberspace? In response to these questions, we need to note the following. First, the governance of cyberspace is still under construction. In particular, cyberspace lacks a single forum or international organization that is responsible for regulating its activities. As a result, governance is spread throughout technical standard setting fora, private sector organizations, civil society groups, states and international organizations. Governance ranges from developing norms and codes of conduct, to signing international treaties and imposing regulations (Nye 2014). Over the past years, there have been attempts both at the national and the international level to address human rights' concerns in cyberspace. States have passed laws and taken initiatives to counter cyber threats, but an international treaty that would regulate activities in cyberspace is still absent. Since 2010, the Groups of Governmental Experts (GCEs) have been appointed by the UN General Assembly to report on the nature of cyber threats and their implications for national and international security. In their reports, the GCEs emphasized that states have to respect human rights and fundamental freedoms when addressing cyber security issues (Green & Rossini, 2015, p. 5). Likewise, in 2013, the European Commission adopted the 'Cybersecurity strategy of the European Union: an open, safe and secure cyberspace' which states that EU's core values apply as much in the digital as in the physical world and that cyber security is only effective when based on fundamental rights and freedoms (2013, pp. 3-4). Despite the above positive developments, there is still no law enforcement mechanism that can ensure the protection of human rights in cyberspace (Mihr, 2014, p. 25, 32). For example, there is no universal consensus on what constitutes personal data in cyberspace. The EU treats IP addresses as part of personal data, whereas the US does not (Inkster, 2014, p. 53). Likewise, in terms of data privacy, the EU applies a strict and top-down regulation system, where governments play a leading role, whereas the US relies more on industry self-regulation mechanisms (Gady, 2014). Another point to consider regarding the protection of human rights in cyberspace is the future demographic trends. Nowadays, only 30% of world population has regular access to the Internet. The next billions of Internet users are coming from states in the Global South that embrace a Westphalian understanding of state and national security. Many of these states have authoritarian and autocratic regimes that have already developed cyber surveillance programs, at the expense of human rights (Deibert, 2013b, p. 9). Pushing the global agenda for a human-centric understanding of cyber security, is not a priority for these states.

Second, in the absence of global governance, the only actor that has the authority and capability to secure human needs is the state (Smith, 2010, pp. 42-3). This is not to devalue the importance of a human-centric approach towards cyber security, but rather to place the discussion in a pragmatic context. This context might involve international and private actors (international community and civil society), but it cannot exclude states. National security by definition includes the protection of a state's territory, sovereignty, and citizens. That notion expresses the reality of the pre-Internet era. Cyberspace is different from the other physical domains (land, sea, air, and space) against which states have to safeguard. Cyberspace is a transnational domain in which states are trying to overcome

the border paradox and exercise their sovereignty (Liaropoulos, 2011). The oxymoron is that in the case of cyberspace, states have the obligation to secure their citizens, but at the same time they make them feel insecure by violating their online human rights. Framing the protection of human rights in cyberspace as a national security issue might be counterproductive, due to its potential for abuse (Comninos & Seneque, 2014, p. 38). States need to realize that citizens should enjoy the benefits of cyberspace and not be targets of massive and illegitimate cyber surveillance. Safeguarding privacy and freedom of expression as well as restricting unjustifiable public-private sharing of personal data should be added to the cyber security agenda of policy makers.

CONCLUSION

Cyber security has been approached by various disciplines. Information technology experts, lawyers, strategists, and state officials have enriched the debate about the nature of cyber security. The dominant trend—regardless of its theoretical origin—is state-centric. The current approach to cyber security is counterproductive and largely irrelevant, if not hostile, to people's needs. Instead of making cyberspace more secure, states are producing cyber(in)security both at the international system and among sub-state actors. As in many others cases in the past, the interests of states has overshadowed the interests of people. Indeed, cyber weapons created to defend a nation's assets in cyberspace are also being turned against its own citizens. Breaking the so-called cyber security dilemma and striking a balance between national cyber policies on the one hand and liberty, anonymity, and freedom of speech on the other hand are incredible challenges.

The dangers entailed by the concept of the 'surveillance state' are not new. The fear is that cyberspace might turn—or has already turned—this ominous metaphor into a reality. In the age of Big Data and the Internet of Things, anonymity is fading away. Companies are using meta-data to shape marketing strategies through personal advertising. The work of national security and intelligence agencies depends on monitoring the full range of human activities in the digital sphere. The securitization of cyberspace is inevitable, but the form that cyber security will take in the near future is not. In reality, the present securitization of cyberspace relates to the securitization of every aspect of our daily lives. Shifting the narrative towards human rights is only the first step in ensuring the protection of internet users. Securing the human needs in a domain that lacks effective governance and blurs the lines between national and international, public and private is a riddle rubbed in a mystery inside an enigma.

NOTE

This publication is a revised version of the paper 'Cyber-security: a human-centric approach', presented at the *14th European Conference on Cyber Warfare and Security*, University of Hertfordshire, Hatfield UK, 2-3 July 2015.

REFERENCES

Bajaj, K. (2014). Cyberspace: Post Snowden. *Strategic Analysis*, *38*(4), 582–587. doi:10.1080/09700161.2014.918448

Betz, D., & Stevens, T. (2011). *Cyberspace and the state: toward a strategy for cyber-power. Adelphi Paper 424*. Oxfordshire, UK: IISS & Routledge.

Booth, K., & Wheeler, N. (2008). *The security dilemma: fear, cooperation and trust in world politics*. New York, USA: Palgrave.

Brantly, A. F. (2014). The cyber losers. *Democracy and Security*, *10*(2), 132–155. doi:10.1080/17419166.2014.890520

Comninos, A., & Gareth, S. (2014). Cyber security, civil society and vulnerability in an age of communications surveillance. In Global Information Society Watch 2014. Communications surveillance in the digital age (pp. 32-40).

Cropf, R., & Bagwell, T. (Eds.). (2016). *Ethical Issues and Citizen Rights in the Era of Digital Government Surveillance*. IGI Global. doi:10.4018/978-1-4666-9905-2

Cukier, K., & Mayer-Schoenberger, V. (2013). The Rise of Big Data. *Foreign Affairs*, *92*(3), 27–40.

Deibert, R. (2012). The growing dark side of cyberspace (…and what to do about it). *Penn State Journal of Law & International Affairs*, *1*(2), 260–274.

Deibert, R. (2013a). *Black code: inside the battle for cyberspace*. Toronto, Canada: McClelland & Stewart.

Deibert, R. (2013b). Bounding Cyber Power: Escalation and Restrain in Global Cyberspace. The Centre for International Governance Innovation; Internet Governance Papers (no. 6). Retrieved from https://www.cigionline.org/sites/default/files/no6_2.pdf

Deibert, R. (2015). The geopolitics of cyberspace after Snowden. *Current History (New York, N.Y.)*, *114*(768), 9–15.

Dunn Cavelty, M. (2012). The militarization of cyberspace: why less may be better. In C. Czosseck, R. Ottis & K. Ziolkowski (Eds.), *Proceedings of the 4th International Conference on Cyber Conflict* (pp.141-154). Tallinn, Estonia: CCD COE Publications.

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, *20*(3), 701–715. doi:10.1007/s11948-014-9551-y PMID:24781874

Epstein, G. (2013), Online and Off, Information Control Persists in Turkey. *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/deeplinks/2013/07/online-andinformation-control-persists-turkey

Etzioni, A. (2015). *Privacy in a Cyber Age: Policy and Practice*. New York, USA: Palgrave Macmillan. doi:10.1057/9781137513960

European Commission. (2013). *Cybersecurity strategy of the European Union: an open, safe and secure cyberspace*. Retrieved from http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

European Parliament. (2015). *Surveillance and Censorship: The impact of technologies on human rights*. Retrieved from http://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf

Gady, F. (2014). EU/U.S. Approaches to Data Privacy and the "Brussels Effect". *Georgetown Journal of International Affairs. International Engagement on Cyber*, *IV*, 12–23.

Green, N., & Rossini, C. (2015). Cyber security and human rights. Public Knowledge. Retrieved from https://www.gccs2015.com/sites/default/files/documents/Introduction%20Document%20for%20GCCS2015%20Webinar%20Series%20-%20Cybersecurity%20and%20Human%20Rights%20(1).pdf

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA and the U.S Surveillance State*. New York, USA: Metropolitan Books.

Hare, F. (2010). The cyber threat to national security: why can't we agree?', In C. Czosseck & K. Podins (Eds), *Proceedings of the Conference on Cyber Conflict* (pp.211-225). Tallinn, Estonia: CCD COE Publications.

Inkster, N. (2014). The Snowden Revelations: Myths and Misapprehensions. *Survival*, *56*(1), 51–60. doi:10.1080/00396338.2014.882151

Jervis, R. (1978). Cooperation under the security dilemma. *World Politics*, *30*(2), 167–214. doi:10.2307/2009958

Klimburg, A. (Ed.). (2012). *National cyber security framework manual*. Tallinn, Estonia: CCD COE Publications.

Kovacs, A., & Hawtin, D. (2013). *Cyber security, cyber surveillance and online human rights. Stockholm Internet forum on Internet freedom for global development*. Stockholm, Sweden: Global Partners & Associates.

Kramer, F., Starr, S., & Wentz, L. (Eds.). (2009). *Cyberpower and national security*. Washington, D.C: Potomac Books & National Defense University Press.

Liaropoulos, A. (2011). Power and security in cyberspace: implications for the Westphalian state system. In M. Majer, R. Ondrejcsak, V. Tarasovic, & T. Valasek (Eds.), *Panorama of Global Security Environment* (pp. 541–548). Bratislava, Slovakia: Centre for European and North American Affairs.

Liaropoulos, A. (2013). The challenges of social media intelligence for the intelligence community. *Journal of Mediterranean and Balkan Intelligence*, *1*(1), 5–14.

Lucas, E. (2015). *Cyberphobia: identity, trust, security and the Internet*. New York, USA: Bloomsbury Publishing.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 1–13. doi:10.1177/2053951714541861

Mihr, A. (2014). Good cyber governance: The human rights and multi-stakeholder approach. *Georgetown Journal of International Affairs*. *International Engagement on Cyber*, *IV*, 24–34.

Mordini, E. (2014). Considering the Human Implications of New and Emerging Technologies in the Area of Human Security. *Science and Engineering Ethics*, *20*(3), 617–638. doi:10.1007/s11948-014-9555-7 PMID:25027858

Morozov, E. (2011). *The net delusion: the dark side of Internet freedom*. New York, USA: Public Affairs.

Nocetti, J. (2015). Contest and conquest: Russia and global Internet governance. *International Affairs*, *99*(1), 111–130. doi:10.1111/1468-2346.12189

Nye, J. S. (2014). The Regime Complex for Managing Global Cyber Activities. The Centre for International Governance; Global Commission on Internet Governance: Paper Series No. 1. Retrieved from https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf

Smith, M. (2010). *International security: politics, policy prospects*. New York, USA: Palgrave Macmillan.

Tavmen, G. (2014). Internet Rights that went wrong in Turkey. In Global Information Society Watch Special Report. Association for Progressive Communications (APC) and Humanist Institute for Cooperation with Developing Countries (Hivos).

Thomas, T. (2010). Google Confronts China's Three Warfares. *Parameters*, *40*(2), 101–113.

U.S House of Representatives, Permanent Select Committee on Intelligence. (2013). *Cyber Intelligence Sharing and Protection Act of 2013.* Retrieved from http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/CISPAPassedApril2013.pdf

Ventre, D. (Ed.). (2012). *Cyber conflict: competing national perspectives*. London, UK: ISTE and John Willey & Sons. doi:10.1002/9781118562666

Williams, P. (Ed.). (2008). *Security studies: an introduction*. London, UK: Routledge.