DOI:10.33179/BSV.99.SVI.11.CMC.13.3.2

Uroš Svete,
Anja Kolak

Izvirni znanstveni članek

VARNOSTNA RELEVANTNOST KIBERNETSKEGA PROSTORA V OBDOBJU WEB 2.0

CYBERSPACE SECURITY RELEVANCE IN THE TIME OF WEB 2.0

Original scientific article

Povzetek Informacijska tehnologija in varnostni sektor sta bila vseskozi povezana, še posebej pomembna pa je razprava postala v času, ko so praktično vse ključne družbene infrastrukture postale odvisne od digitalne tehnologije. V tem članku smo z uporabo varnostnih teorij analizirali pomen kibernetskega prostora, pri čemer smo posebno pozornost namenili razvoju druge generacije svetovnega spleta (in v tem okviru posebej primera WikiLeaks), pri katerem so nosilno vlogo pri proizvodnji podatkov in informacij prevzeli uporabniki sami. Internet je tako res postal komunikacijska hrbtenica, prek katere so povezane množice uporabnikov, tako komuniciranje pa (zahodnim) državam predstavlja vse večji izziv, včasih celo grožnjo njihovi nacionalni varnosti.

Ključne besede ***Informacijsko-komunikacijska tehnologija, kibernetski prostor, sekuritizacija, Splet 2.0, WikiLeaks.***

Abstract Regardless if the information-communication technology has been developed to follow national security interests or not, at the moment, nobody doubts this correlation anymore. But the discussion has become much more important in time when practically all critical social infrastructures and processes depend on digital technology. In the paper, importance of the cyberspace has been analysed by security theories and with special focus on the Web 2.0 and WikiLeaks issue. The current way of such interactive communication is namely based on individuals as data and information producers, which could be in (Western) countries perceived as a greater challenge and in some cases even national security threat.

Key words ***Information and Communication Technology, cyberspace, securitization, Web 2.0, WikiLeaks.***

Introduction

Throughout human history, technological and technical revolutions have also had security dimensions. However, none of them have changed the power relations in a way the information and communication technology (ICT) and related information revolution has. We often think that the Cold War period was mainly marked with (nuclear) arms race and war for resources in a physical (real) space[1]. However an increasing number of authors have looked for reasons for a well-known result of this era and the supremacy of the western world[2] within the development of information technology and its impact of weapons systems as the ways of the functioning of military and non-military organisational structures (Štrubej, 2008, Klimburg, 2011). Despite varying explanations of the reasons and intentions which had resulted in the predecessor of Internet, ARPANET[3], there is today broader consent on the fact that the expansion of ICT and the appearance of cyberspace[4] have undoubtedly fundamentally changed practically all social subsystems as well as the role of an individual in them. Regardless of how we estimate the developments in late 1950s and early 1960s which have resulted in the informatisation of the world, there is no doubt that cyberspace and security sector have been connected from the very beginning, both in theoretically conceptual and empiric sense. Their relation has been inversely deductive throughout the process. The development of technological capabilities and components has inspired theoreticians (think-tanks) for developing the concepts. However, an inverse relationship is also in place, where several information and cyber operations ideas and concepts have only appeared recently. Although in the recent decade, there has been much writing on ICT security implications in Slovenian scientific and professional world as well, this paper would like to emphasize some new effects characterised for digitalised society. Main focus will be put on the part of the cyberspace development called Web 2.0 as well on security-oriented discussions mainly related to the developments concerning the WikiLeaks "affair". The latter has brought attention back to an individual user and making ICT a real socially technical network (Kling, 2000), where *we're living through reverberations in the form of numerous social media sites and activities that have contributed to nontrivial changes in how w*e learn, play, socialize, entertain, engage with our governments (Davis, 2011, p. 92). On the other hand, it has also underlined the dialectics which

---

[1] *In 1948, international relations theorist, Hans Morgenthau (1904–1980) theorized that national security depends on the integrity of a nation's borders and its institutions (Morgenthau in Geers, 2009, pp. 1).*

[2] *Unlike the American planners who saw the US military benefiting from this silicon revolution, the Soviets were worried about their own economic inability to exploit the digital revolution. The USSR was rapidly losing ground to US prowess in microelectronics (Hughes, 2010, pp. 527).*

[3] *Charles Herzfeld, ARPA Director (1965–1967) argued The ARPANET was not started to create a Command and Control System that would survive a nuclear attack, as many now claim. To build such a system was, clearly, a major military need, but it was not ARPA's mission to do this; in fact, they would have been severely criticized had they tried. Rather, the ARPANET came out of our frustration that there were only a limited number of large, powerful research computers in the country, and that many research investigators, who should have access to them, were geographically separated from them (http://arpanet.co.tv/).On the other hand, Štrubej (2008) sees main initiators of developing the aforementioned network in the tendency to establish a control and communication network capable of surviving a nuclear attack.*

[4] *Cyberspace is the electronic medium of computer networks, in which online communication takes place. The world was first used by William Gibson (http://www.wired.com/science/discoveries/news/2009/03/dayintech_0317) and cyberspace is comprised of both a material and a virtual realm—a space of things and ideas, structure and content (Deibert and Rohozinski, 2010a, p. 16).*

was unimaginable in early 1960s – the very contradiction between a state and its citizens, which nowadays mainly reflects in asymmetry (disagreement) of security concepts, instruments and interests. The example of WikiLeaks is not the only one related to the security of information networks or computer security in a narrow sense. We consider it just as a beginning of the battle for control over ICT users, which will in the future be led by states, non-state (commercial) actors and groups of people with good information technology ability and awareness. Another example, which has in the recent time undoubtedly captured attention, is the ability of destructive use of ICT, which threatens the functioning of critical social infrastructure[5] even when it has no direct access to the Internet. Such case is Stuxnet worm which mainly affected industrial facilities using Siemens Win CC or PCS7 software. It activated itself only if computers were fitted with the mentioned software, which makes it obvious that the aim was not to target a wide circle of usual users, but specific industrial facilities (W32.Stuxnet Dossier, 2011)[6]. Both of the mentioned examples prove that cyberspace is really gaining strategic importance, both, by directly influencing our perception of the environment (also in the sense of security) and by fundamentally changing the functioning of traditional security actors.

Even though, in Slovenia, such discussions used to be perceived with mistrust, scepticism or even ridicule, such realistic examples of cyberspace threats, its influence of the redistribution of social power and, last but not least, the inclusion of the issue in the NATO's New Strategic Concept and the work of the EU[7] force us to seriously address this issue, both, academically and within state authorities and not to keep it just on the paper at the highest strategic levels[8]. Estonia is a good example of how cyberspace perception is not (always) related to financial resources and how even small countries can establish themselves as information security agenda setters.

1 CYBERSPACE IN A SECURITY DISCUSSION

From the very beginning, cyberspace and ICT in general have been closely related to the (national) security sector. However, more precise concepts were not developed until several decades later, when ICT entered practically all social spheres.

---

[5] *Critical infrastructure owners and operators report that their networks and control systems are under repeated cyber-attack, often from high-level adversaries like foreign nation-states. And these kinds of attacks on critical systems such as gas, power and water have increased around the world in last few years (In the Crossfire Critical Infrastructure in the Age of Cyber War, 2009).*

[6] *Stuxnet is a threat targeting a specific industrial control system likely in Iran, such as a gas pipeline or (nuclear) power plant. The ultimate goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries. Stuxnet was discovered in July, but is confirmed to have existed at least one year prior and likely even before. The majority of infections were found in Iran (W32.Stuxnet Dossier, 2011).*

[7] *OPINION of the European Economic and Social Committee on the 'Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) (2011).*

[8] *Nevertheless, it is commendable that cyber threats and abuse of information technology and systems have been explicitly mentioned in the latest Resolution on the National Security Strategy of the Republic of Slovenia ReSNV-1, 2010).*

Although top authorities of the US Department of Defense were aware of the significance of information technology and its role in Revolution in Military Affairs[9] as early as in 1960s and 1970s, more precise information warfare concepts had not been developed until a while later (Hughes, 2010). New strategies and tactics for the pursuance of their aims have been described under the umbrella term 'information warfare'. Although the doctrine of information warfare has emerged from work by researchers and military strategists of the RAND Corporation (Arquilla and Ronfeldt, 1999), it has been used to describe the strategic transformation of the network society also by other kinds of thinkers including social critics, computer scientists (Denning, 1998), business strategists (Munro 2009) and political theorists (Der Derian, 2000). The US approach to the so-called strategic evaluation of ICT has from the very beginning been very defence- and military-oriented. However, it has involved technical personnel as well as social science experts and it has soon been established that strategic use of ICT will have to involve more than just the civil society.

The weapons of information warfare have been developed and refined in both the military and civilian realms of society. Indeed, the theorists of the RAND Corporation note that with information warfare the military and civilian realms have become blurred. The doctrine of information warfare is somewhat broader and more ambitious than simple misinformation and propaganda, although these latter techniques have an important place in the information warfare arsenal. Information technologies and communications networks are the weapons and the targets of information warfare operations. Techniques of information warfare can involve both high and low technology weapons, but it has only emerged as a distinct doctrine in association with the use of relatively hi-tech equipment such as computers, satellites and the Internet. The range of hi-tech weapons includes techniques such as computer viruses, hacking, identity theft, email bombs, phishing and the creation and destruction of websites. Low-tech weapons have been described by the hacker Kevin Mitnick as 'social engineering', but may also include more mundane aspects of social life such as pamphleteering and the spread of rumours. In short, it uses information to undermine and disorientate an adversary, disrupting their ability to effectively mobilize their resources (Munro, 2009, p. 200). In the recent period, USA go even one step further and according to some reports the US is set to publish plans that will categorize cyber-attacks as acts of war against US. In future, a response to a cyber-incident or attack on the US critical infrastructure would not necessarily be a cyber-response. All appropriate options would be on the table and a US president could consider economic sanctions, cyber-retaliation or a military strike if key US computer systems were attacked (Pentagon to treat cyber-attacks as 'acts of war', 2011.)

[9] *In the early 1970s the innovative thinker Andrew Marshall was recruited from the RAND Corporation (Research and Development) by the US Department of Defense to head its Office of Net Assessment. At the Pentagon, Marshall was given the tall-order task of finding ways for NATO to defeat the Warsaw Pact short of a nuclear response. In his first departmental report Marshall told of the progress that US weapons labs were making on a new generation of 'smart' weaponry that would deliver substantially increased lethality with a lower loss of US life. The increased precision was made possible by a new generation of software and electronics built around the microprocessor (Hughes, 2010, pp. 526-527).*

While the number of ICT users grows and ICT is becoming gradually demonopolised and commercialised, the concept of information warfare is becoming increasingly focused on offensive and defensive operations of armed forces. However, there is, on the other hand, a concept of (strategic) cyberspace and its defence, since people and their ideas and knowledge have truly become an integral part of information and communication technology[10]. Security discussions have split in this respect as well.

Taking note of what has been said over the past few years about the mission of computer security, two conceptions seem dominant. One, here labelled ‘‘technical computer security,’’ has its roots in the scientific and technical field of the same. The other, here labelled ‘‘cyber-security,’’ a more recent entry to the public sphere, is typically articulated by government authorities, corporate heads, and leaders of other non-governmental sectors. It links computer security to traditional notions of national security. At present, these two conceptions exist side-by-side, each one angling for the attention of key social actors including government agencies, technical experts and institutions, corporations, policy experts, pundits, the general public, and, importantly, the media (Nissenbaum, 2005, p. 63). On the other hand, the term ‘cyber warfare’ is used to indicate broadly any warfare waged by states and significant non-state actors in cyberspace. It can include defending information and communications systems, critical infrastructures, weapons systems or military command centres from attack, as well as conducting equivalent offensive operations against an adversary. It does not refer to recreational or socially motivated hacking or ‘hacktivism (Hughes, 2010, p. 525).

If, on the one hand, the US view of cyberspace from a security perspective is still more or less state-centric and realistically oriented in a defence and military sense[11], we cannot avoid the Copenhagen school across the Atlantic and the third (critical) perspective of dealing with modern security issues. The latter is particularly important for our discussion, because it considers two extremely important changes also caused by the informatisation of modern societies. The first one is greater particularisation of security interests and lack of unity between a state and its citizens, while the second one is the complexity of modern security environment. Both can, in our opinion, be understood only if we are precisely aware of social consequences of informatisation which nowadays includes at least half of all humankind.

In proposing a constructivist framework, Buzan and Waever are less concerned with providing an objective characterization of threats, vulnerabilities, and modes of defence, and more with providing a systematic account of the ways specific conditions, states-of-affairs, or events are posed by significant social actors as threats to

---

[10] *Crowdsourcing as a concept as well as a practice refers to the idea that the Web can facilitate the aggregation or selection of useful information from a potentially large number of people connected to the Internet. Wikipedia and, more recently, WikiLeaks are good examples of this distributed knowledge gathering and organization in action (Davis, 2011, p. 92).*

[11] *We are, of course, aware that, in pursuit of this aim, the US is trying to mobilise all social resources. This »whole of nation« approach to security policy – the joint integrated application of state (whole of government) and non-state (business and civil society) efforts to attain common objectives – has only recently begun to be applied in US government circles (Klimburg, 2011, p.43).*

security and come to be widely accepted as such. They call this rendering of a security threat ‘‘securitization,’’ which becomes the fundamental explanatory construct of their framework. The concept of securitization generalizes certain elements of traditional approaches to national security in which the typical landscape includes a threat of military attack, the nation-state under threat, and the specific steps leaders take to ensure the state’s continued security (through such means as defensive action, shoring up vulnerabilities, and so forth.) The Copenhagen School moves from this landscape to the one in which the threat need not be military and the referent object need not be the state (Nissenbaum, 2005, p. 66).

1.1 FROM NATIONAL AND STATE TO HUMAN SECURITY APPROACH

The next very important theoretical framework for understanding security relevance of nowadays cyberspace is also a move and spreading of security actors and threats as well. Instead of the fact that traditional security threats have been rearticulated, the following debate allowed also for treating cyber threat as a constitutional part of modern security at national as well as individual, and even international level.

The (national) security overview in recent decades has shown the prevalence of two main approaches in particular: the traditional (deterministic) and post-modern (complex). For the first, security is the absence of an external threat, or better put, military means should be used for confronting (external) threats. This approach justifies national security as a legitimate way for organizing violence within or between states, but not in any case beyond that (Malešič, 2004). The state has a central role in these security debates; on the other hand it ensures its security interests within the framework of an anarchic and hierarchic international environment, above all using military means or military power (Waltz, 2000). In this sense a traditional security approach is typically realistic. It prevailed during the Cold War and was a theoretical base for simplistic, but very important explanations of wars, alliances, imperialism, blockades and other important international topics (Walt, 1998).

The other main concepts, developed in the Cold War period and based on the starting points mentioned, are common security, stable peace and security approaches in the Third World. Although these concepts go beyond our discussion, they have some very important implications for moving security attention from the state to an individual level. While the common security project was the outcome of political élites, the stable peace concept arose from academic research of peace, based on Galtung’s and Boulding’s analyses. In this sense, peace could not be considered as the absence of war but as a state of society, which ensures the requisite conditions of social justice. Therefore Galtung (Bilgin, 2003, p. 204) differentiates between personal and structural violence. Equally, he divides negative peace as absence of armed conflicts from positive peace as absence of direct (physical) and indirect (structural and cultural) violence. To achieve positive peace, dialogue, cooperation and solidarity among peoples have to be re-established. It is understandable that Galtung and other authors redirected research focus from the state and military dimension towards individuals and social groups (Bilgin, 2003, p. 204-205).

In the 1960s, more complex definitions of national security appeared. According to the liberal and especially the constructivist critical security theory, the foci and security agenda had moved from the national state level towards non-state actors. But the new security understanding ("new security") did not acquire significant legitimacy until the end of the Cold War, when human beings/individuals as reference objects of security had been exposed to the collapse of the static bipolar world order and influence of the globalization (the concept of human security) (Newman, 2001). On the other hand, the legitimacy of discussion about security subjects (whose security?), security emancipation and insecurity dilemmas (butter or guns, individual vs. state/nation etc.), as well as societal/human security and risk society, is increasing significantly. These can be paraphrased or described by social development trends such as growing economic and political inequalities within particular national states as well as between them, a lack of natural resources, migration problems, the spreading of intrastate conflicts, undermining of international peace and stability, and technological challenges. These are just some of the agenda-setting issues or issues that traditional security paradigm is not in position to face. Within this framework, more complex security definitions should be understood (Bilgin, 2003). Security – whether or not one insists on a distinction between 'hard' and 'soft' security – is about more than protecting a country from external threats; security may well include critical infrastructure protection, economic, social security, environmental and human security (Liotta, 2002, p. 475). Security is therefore a matter of feelings and a matter of our physical environment perception.

Following thesis may be too bolt, but without informatisation, the decentralisation of modern societies would not be as fast and it is a big question, if the societies had even wanted such way of social development. While self-initiative and private initiatives in the US have been crucial for the development of ICT, individualisation has also significantly changed security perspectives. Since security implications of ICT can be divided into direct ones (when the use of ICT makes changes in the perception of reality and, consequently, threat) and indirect ones (working of traditional security instruments and mechanisms has been changing by the use of ICT) (Svete, 2005), it is completely understandable why such a large concept and theory apparatus is needed. This is particularly true with regard to the security analysis of the part of ICT development, which we call Web 2.0 and which will logically be followed by the Internet of Things, when, in addition to the humankind, practically all electronic devices will be interconnected[12]. If, in the initial phase, the Internet was complex merely due to its technical component enforcing the principle of decentralised action, the second phase is linked to complexity arising from the transformation of millions of ICT

[12] *"A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communications capabilities. This infrastructure includes existing and evolving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent federated services and applications. These will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability." (CASAGRAS, an EU Framework 7 Project, 2009). The evolving vision of Web 3.0 (sometimes referred to as the service Web) is based on the balanced integration of diverse services provided by human agents and machines over the World Wide Web. This is also the intuition that drives crowd-servicing, which lets us create platforms on which we can build new applications and even enterprises (Davies, 2011, p.93).*

users from readers, spectators and listeners of electronic media into active users and producers of multimedia information capable of real-time transfer and use. Davis (2011) in such cases uses the term 'crowdsourcing' denoting users (the crowd) as the main source of information.

2 CYBERSPACE COMPLEXITY AND SECURITY DILLEMA IN WESTERN DEMOCRACIES

As it has been mentioned, cyberspace is a global and extremely complex web of electronic devices and users with Internet access having a wide variety of aims and interests. It is therefore completely logical that the reaction to providing of security, both from a national and individual perspective, has to be complex and comprehensive. But is this really the case?

Although, in theory it is clear enough that the cyber security problem does not fit conventional or traditional security categories based on individual security responsibilities, economic or corporate security issues, military security problems, as well as domestic versus international problems, the practice is not so concise. Hence, domestic law enforcement must interface with military defence information warfare operators. In addition to that, cyber security is non-geographic; therefore the notion of territorial divisions of responsibility makes little sense. Computerized information flows around the world, investigators of each country like the Federal Bureau of Investigation or other national polices must thus increasingly cooperate with foreign law enforcement agencies to solve cybercrimes[13] (Harknett and Stever, 2011, pp. 455-456). There have, however, been several attempts, especially at a national, but also international level, using reformed and adjusted, but still traditional security mechanisms to deal with contemporary challenges. And at that point we notice the entire scope of different concepts of, both, cyber threats as well as corresponding responses. Deterrence, civil defence, collective defence, and arms control were key national security doctrines in the 20th century, and they are being revaluated now for application to cyberspace (Michael, Tikk, Wahlgren, Wingfield, 2010, p. 91). But is this even possible? As it will be evident later on (especially in the case study on WikiLeaks and the responses to it), it was especially the western countries that found themselves in a great dilemma. On the one hand, they have been accelerating the development and dispersion of information technology for several years, trying to obtain world supremacy in economy, politics, culture and security. For western democracies, the most important dimension of cyber power is thus the ability to motivate and attract their own citizens, an inward focused soft-power approach that is fundamental for creating "whole of nation cyber capability (Klimburg, 2011, p. 43). On the other hand, their critical infrastructure is becoming increasingly dependent on ICT. Considering the fact that we have recently witnessed a vast increase in threats to information critical infrastructure posed, both, by other countries and individuals

[13] *As an example we can put out also Maribor's group of crackers (computer criminals), responsible for developing a virus that breaking into credit cards numbers and other confidential data made possible. This case was investigated by FBI and Slovenian police.*

(whose interests may be purely personal or who may for various reasons link up at an international level), it is perfectly logical that cyber security has become a common topic in lay, professional and political public. There is no more doubt that cyberspace access has grown to become a national security concern in most nations because of the integral role that information and communication technology (ICT) plays in most aspects of private and public affairs. Actions against this critical infrastructure can be criminal, requiring a law enforcement response; involve espionage, which demands action by a country's intelligence community; or even come in the form of an armed attack that permits military self-defence by a nation's armed forces (Michael, Tikk, Wahlgren, Wingfield, 2010, p. 91). In this respect, it is interesting that an increasing number of cyber security initiatives see solutions in an international agreement and cooperation among countries. In today's interconnected networks, (cyber) threats can originate anywhere. Therefore national, regional and international co-operation and coordinated action is needed to address cyber security-related issues (Sund, 2007, p. 571). Hughes (2010) proposes that a multilateral regime is needed to govern cyber-warfare at the global level. As the prospect of a prolonged interstate cyber-war increases, this article examines the role that a cyber-warfare treaty or 'Treaty for Cyberspace' could play in limiting the adverse human effects of interstate conflict in cyberspace. Without this kind of consensus the world may indeed be witnessing not only the rise of a new zone of strategic competition but, more consequentially, ground zero for the next global arms race[14]. Such kind of proposals have been supported also by Geers (2010b) who's idea is Cyber Weapons Convention according to good results brought about by 1997 Chemical Weapons Convention (CWC). The aforementioned approach is therefore trying to respond to cyber threats with an international agreement as an instrument of collective security which would limit or even inhibit the arms race in cyberspace. A problem arising thereof is a technical or legally normative limitation of users' freedom which has throughout the process been the motor of ICT development.

The second interesting example is the securitisation of cyberspace and threats within NATO, which should transform from a Cold-War form (1.0) into a second-generation security organisation (2.0). The widely publicized attacks on Estonian networks in 2007 and Georgia's state systems in 2008 have been attributed either to Russian patriotic hackers or to official Russian agents. NATO responded to the Estonia network shutdown by convening an emergency meeting of the North Atlantic Council; and at the 2008 Bucharest summit, the alliance announced its first cyber-defence policy, marking the first occasion on which an international military organization had deemed cyber-security to be a collective defence obligation. NATO claims that, should a member state face a catastrophic cyber-attack, its new cyber-security

[14] *By the start of 2010 China, India and Russia alongside the US, the UK and South Korea are among the first group of countries to establish formal command and control (C2) over military assets in the cyber-domain. In addition, a host of non-state actors are engaged in cyber-warfare. Al-Qaeda, Hezbollah, Hamas, Zapatistas and a variety of 'patriotic' hacker-attackers are just some of the known paramilitary, resistance or revolutionary groups that have used cyber-warfare or plan to engage in it, with or without specific state sanction. As numerous media accounts have attested, even a teenager armed with a consumer PC and a broadband connection can wreak havoc on both business and government organizations in cyberspace, as demonstrated in 1999 by teenage British hackers who altered British military secure satellite orbits (Hughes, 2010, p. 524).*

policy gives it the tools to respond effectively (Hughes, 2010, p. 529). Also Myrli (2011, p. 87) found out the cyber threats become global therefore every successful security mechanism would need cooperation. But at the same time he is aware of complication factors. Much of the vulnerability to cyber-attack stems from a lack of preparedness in both the governmental and private sectors. Over 50% of industry insiders and other experts from the US, Europe, and Canada said that utilities, oil and gas, transportation, telecommunications, chemical, emergency services, and postal/shipping industries were not prepared for a cyber attack. However, the anonymity enjoyed by cyber aggressors adds a deeply complicating dimension to the nature of the threat. Unlike the telephone system, which has an effective tracking and billing capability based on the need to charge users, the Internet was designed as an open and robust system for the sharing of information, and therefore has no standard provisions for tracking or tracing the behaviour of its users. And last but not least competition exists. Though emerging threats to some extent could compel players to cooperate, the global security situation is still complicated as nations or blocs are vying mainly for their own benefits. The case is the same with NATO. While claiming that it does not consider any country to be its adversary, NATO still puts deterrence as a core element of its overall strategy.

The challenge of cyber security is both significant and complex. Achieving effective regulatory governance in this area calls for a comprehensive strategy that involves coordinated action by government, the private sector, and individual citizens. Of course, an undertaking of this size and magnitude cannot be completed overnight – it requires a sustained, multi-year effort with significant governmental and private sector cooperation (Chertoff, 2008, p. 484). However did we already reach such kind of security development? More likely, we could concur with the finding of Deibert and Rohozinski (2010b, p. 44) that pointed out rather than being an ungoverned realm, cyberspace is perhaps best likened to a gangster-dominated version of New York: a tangled web of rival public and private authorities, civic associations, criminal networks, and underground economies. After all, this establishment is also supported by dilemmas relating to the provision of information security, which increasingly appears to be the victim of discrepancy between state interests and specific interests. In this respect it is more than obvious that mainly western democracies somehow have problems determining the boundary between the freedom of ICT use and the threat to (national) security. The USA and many other western democracies thus, on the one hand, support informational freedom in the countries like China, Iran and Arabic countries, mainly in the use of the second-generation social networks on the World Wide Web, but on the other hand limit this very freedom, when their national security and strategic priorities are threatened. It is this dilemma that we find as one of the crucial ones to impact further ICT development. In a technical sense, this web will be much harder to control, especially after the transfer to the Internet Protocol version 6, because the number of connected devices will increase rapidly. In the end, it will be possible to achieve information security only by physically disconnecting the network, which some dictators in Arab countries have already attempted. And we know how they ended up. Since in such events, the mobilisation power of

social networks and their influence even on social processes became evident, we will focus more on the second-generation web and the Wiki platform which started a real "cyber war" between its supporters and opponents. There is, however, one other important dilemma supported by Deibert and Rohozinski (2011). They draw attention to the fact that, in the information age, we leave digital traces practically everywhere, copying our analogue lives into the binary code. Digital information can easily be tracked and traced, and then related to specific individuals who themselves can be mapped in space and time with a degree of sophistication that would make the greatest tyrants of the past days envious. So, are these technologies of freedom or are they technologies of control? This goes especially for the rise of social networks, such as the Facebook, and the platforms abiding by cloud computing (Google, Apple, Microsoft). And, in terms of their value and influence, these brands belong to the top companies, at the same time shining out the cyber power of the USA, which its main allies, competitors and opponents are well aware of.

2.1 THE SECOND-GENERATION WEB

In contrast to the first generation of the development and use of the Internet, which was mainly used in the same manner as the traditional media (characteristic of them is a one-way data flow), the biggest revolution occurred with their engagement and cooperation in the development of services and their contents. Web 2.0 thus benefits from the biggest advantage of the Internet infrastructure, i.e. its interactive use, which of course requires an active user.

The most significant characteristics that a core 'Web 2.0 service' follows (http://www.techpluto.com/web-20-services/):

- **User-centred Design**. A web design which is created in a way that it fulfils every possible need of the end user and empowers the user to perform certain customizations within the design. User-centred designs are cleaner, often Ajax based and easy to navigate. The appearance of the design is given a special preference while creating such a design. iGoogle, a customizable Google homepage is one of the most appropriate examples of a User-centred design.
- **Crowd-sourcing**. Every small unit of contribution is important to a Web 2.0 service. Millions of such contributions eventually lead the website to state of higher relevance. For instance, any conventional Media company (employing hundreds of reporters) has today been easily beaten by blogging platforms like Blogger and WordPress in producing extremely frequent and relevant content as millions of users are acting as a contributor, building up a large resource within much lesser span of time.
- **Web as Platform**. Gone are those days when one had to heavily rely on the desktop for accessing various web applications. Today's Web 2.0 services don't require a client download condition. Nor is the dependency on a particular OS for accessing the web services. Whatever be the method of internet access (Windows, Mac or Mobile OS), the Web 2.0 applications are nowhere affected by it.
- **Collaboration**. Wikipedia takes the first place when it comes to proving the power of collaboration. Before 2001 (year of Wikipedia's inception), there used to exist

only driven information sources such as Britannica Encyclopaedia, where collaboration was never implemented. Today, Wikipedia stands way ahead in terms of content quantity as well as quantity.
- **Power Decentralisation**. Earlier, most of the services used to be administered and not automated. But Web 2.0 services follow a self-service model rather than being administrator dependent. For instance, Google AdSense is a self-service platform for Ad publishing. There is no administrator for allowing/rejecting the requests from the users. The users get to have a self-service system by Google which helps them deploy Ads on their site/blog quite easily.
- **Dynamic Content**. In a generation where blogosphere has overpowered the conventional mainstream media, Web 2.0 services have to be highly dynamic and proactive. If crowdsourcing is there then dynamicity follows by default.
- **SaaS**. With Cloud computing on a roll, more and more web services are taking the route of SaaS (Software as a Service). Software is available as a web service with no platform dependency at all.

2.2 WIKILEAKS

Although a lot of services based on Web 2.0 have been developed, from security point of view, particularly one has to be emphasized. In this chapter, we introduce Organization WikiLeaks which has gained international attention after posting classified documents and reports of governments, corporations and other high-profile organizations all over the world. WikiLeaks disclosed from security perspective sensitive diplomatic and military activities with an intention to make them transparent. The consequence was an increased gap between the citizens and states. WikiLeaks announcements were also a trigger for the "first cyber war" between organisation supporters and opponents, where also a part of critical infrastructure has been affected. There is no doubt; WikiLeaks caused tremendous changes in security sector as well in the role of a Western state and its citizen. Therefore, cyberspace security relevance in the time of Web 2.0 got an absolutely new dimension.

WikiLeaks is an international non-profit media organization which publishes news leaks based on their ethical, historical, diplomatic and political significance. Organization provides an innovative, secure and, most important, an anonymous way for sources to leak information to journalists, newspapers and to the general public (WikiLeaks, 2011). WikiLeaks operates, communicates and interacts with the outside world via the website known as Wikileaks.org. "Website that defines itself as a public service designed to protect whistle-blowers, journalists and activists who have sensitive materials to communicate to the public", came online on October 4, 2006 (Fogarty, 2010, p. 5). Since the website went online, it has posted an extensive catalogue of secret and classified material such as: e-mails from the University of East Anglia, in England – also known as 'Climategate', classified US military field reports from the War in Afghanistan – 'Afghan War Diaries', reports from War in Iraq – 'The Iraq War Logs' and U.S. State Department diplomatic cables – also known as "Cablegate" (Khatchadourian, 2010).

WikiLeaks: Complete Transparency?

The website WikiLeaks.org was originally created online in wiki[15] format, but gradually it has modified to a more traditional and restrictive publication model, so the documents cannot be edited by random readers (Steller, 2009). WikiLeaks describes itself as "an uncensorable system for untraceable mass document leaking and public analysis" (Khatchadourian, 2010). Documents and multimedia files can be leaked on a massive scale in a way which "combines the protection and anonymity of cutting-edge cryptographic information technologies" (WikiLeaks, 2011). According to Julian Assange and co-workers, they use their own coded software combined with OpenSSL[16], FreeNet[17], PGP[18] and Tor[19] as a main anonymity protection device (Leigh, 2011, pp. 52-53). According to Fenster, "WikiLeaks has established a powerful brand identity as a technologically sophisticated service capable of distributing data anonymously and publicizing its release." The success of the WikiLeaks has inspired also other supporters around the world and similar sites started to open, all patterned on the WikiLeaks model (Fenster, 2011, p. 7) (e.g., OpenLeaks.org, BrusselsLeaks.com, Transparency.AlJazeera.net).

WikiLeaks collects and publishes material that has been classified as confidential by corporations or government agencies. The idea of the organization is simple and clear: *complete transparency in politics and economy,* says Julian Assange (Kämmerling, 2011, p. 11). The website of WikiLeaks gives all the necessary information and directives to the potential informers how to hand over various documents or other materials.

---

[15] *The wiki concept was developed in 1995 as a collaboratively built site where content can be added or edited by any user. »It is web-based software that allows all viewers of a page to change the content by editing the page online in a browser. » (Ebersbach, 2008, p. 12). A wiki is a set of linked web pages where everyone has rights to edit everything, and editing is not discouraged but encouraged. Wikis are used to share general information with targeted audiences and to support collaborative work, such as projects or reports. In addition to text, wikis can feature text, graphics, video clips, and even plug-ins. Primarily due to the success of the free online encyclopaedia Wikipedia – The Free Encyclopaedia', wikis have become known to a wide audience (Ebersbach, 2008, pp. 13-14). Wiki is known as one of the key tools in Web 2.0.*

[16] *OpenSSL is an open source secure site connection system. It is a popular open source implementation of the SSL/TLS protocols. OpenSSL uses various cryptographic algorithms to ensure secure communication: symmetric key (secret key) encryption, asymmetric key (public key) encryption, message digests/digital signatures and certificates (http://www.openssl.org/).*

[17] *Freenet is free and open source software which operates as a location-independent distributed file system across many individual computers that allows files to be inserted, stored and requested anonymously (http://freenetproject.org/index.html).*

[18] *PGP – 'Pretty Good Privacy' is open source cryptographic system, to provide a secure communication in an insecure electronic environment (http://www.pgpi.org/).*

[19] *Tor - 'The Onion Router'is a sophisticated privacy tool that lets users navigate and send documents through the internet anonymously. It is a network of virtual tunnels that allows people and groups to improve their privacy and security on the internet. It was a US Naval Research Laboratory project, developed in 1995, which has been taken up by hacker around the world. It uses a network of about 2.000 volunteer global computer servers, through which any message can be routed, anonymously and untraceably, via other Tor computers, and eventually to a receiver outside the network. The key concept is that an outsider is never able to link the sender and receiver by examining »packets« of data (Leigh, 2011, p. 52-53).*

Anonymity as informant's top priority

There are four different ways in which an informant can hand over secret material to WikiLeaks:

a) *Via postal drops* (as an alternative method); digital copies on a data storage device or printouts sent to a P.O. Box in Australia by regular mail.
b) *In person;* the informant or intermediary hands over the document and video files to a WikiLeaks operator.
c) *Anonymous electronic drop box* (the preferred method of submitting any documents):
   – The informant uploads data through public internet access point (an internet café), the data is encrypted and transmitted to WikiLeaks (SSL encryption).
   – The informant uploads the data from his computer via the gateway network. This process involves cloaking the data's origin as well as providing counter-measures against bugging (SSL encryption).

After receiving the material, WikiLeaks operators remove any digital traces that would lead to the data's source and verify authenticity of the documents (they publish only original documents). The secret documents are fragmented into data packets distributed over numerous servers all over the world only to be reassembled on the reader's PC. WikiLeaks mirrors are accessible via hundreds of internet addresses. Redacted documents from WikiLeaks are first received by the publishers and journalists. Regular internet users can enter an operational WikiLeaks address and an upstream server, which does not store the data itself, but connects them to one or several other available servers (from WikiLeaks to the reader with SSL encryption). (WikiLeaks, 2011, Kämmerling, 2011, p. 12).

Breakthrough: Posting secret data

In January 2007, WikiLeaks announced 1.2 million documents waiting to be processed and published. A huge breakthrough and first major release was on April 5, 2010 when WikiLeaks released a classified US military video footage (entitled as "Collateral Murder") of a US Apache helicopter shooting into a crowd in Bagdad in 2007 which killed 12 people, including two Reuters journalists (http://www.collateralmurder.com/). The next release was on July 25, 2010, when WikiLeaks released more than 91,000 reports covering the war in Afghanistan from 2004 to 2010. Classified military reports called 'Afghan War Diaries', providing insights into unreported civilian deaths, secret operations against the Taliban, U.S. fears that Pakistan's intelligence service was aiding the Afghan insurgency, etc. On October 22, 2010, WikiLeaks released a package of 391,000 documents called 'The Iraq War Logs', with a focus on Iraq War between 2004 and 2009 (Zumwalt, 2010).

On November 28, 2010, WikiLeaks released approximately 250,000 documents, focusing on U.S. State Department diplomatic cables. According to BBC news "the diplomatic cables cover messages sent between 1966 and 2010 and originate from 274 US embassies, consulates and diplomatic missions." The entire archive of the

reports has been made available to five world-class news organizations: *The Guardian* (United Kingdom), *El País* (Spain), *Le Monde* (France), *Der Spiegel* (Germany) and *The New York Times* (United States) (BBC, 2010).

DDoS attacks

The response to the WikiLeaks US diplomatic cables release was dramatic and even more interesting. After the release of the documentation, WikiLeaks' website suffered disabling denial-of-service (DDoS[20]) attack. Cross-system attacks to servers tried to prevent the material from spreading throughout the internet. The hacker behind the attack appeared to be a patriot-hacker called "The Jester", describes himself as a "hacktivist for good" (Leigh, 2011, pp. 203-204). In response to the dissemination of classified documentation, the U.S. government began to exert pressure on organizations linked to WikiLeaks. The Amazon[21] which was hosting computer space to WikiLeaks and EveryDNS which provides free domain names dumped their client. A second type of systems that came under attack on a model parallel to the attack on technical infrastructure was payment systems. Shortly after the cables were published, several financial institutions, including *PostFinance*, *the Swiss postal system, PayPal*, *Bank of America, Visa and MasterCard*, closed Assange's and WikiLeaks' accounts[22]. None of these actions proved disabling. Hundreds of other servers around the world started hosting 'mirrors'[23] (copies of the site), the website was quickly up and running again using the Swiss domain named Wikileaks.ch. (The Economist, 2010). Some government departments and server providers have banned WikiLeaks in their countries, such as Australia, Switzerland (by a US service provider) and United States Military (Lennon, 2010).

After all 'government actions' against WikiLeaks, a group known as Anonymous launched DDoS attacks against websites operated by organizations opposing WikiLeaks. As a consequence of this attack Facebook and Twitter also closed the accounts and pages used by Anonymous (The Economist, 2010).

Anonymous strikes back

Online activists calling themselves Anonymous (AnonOps) have launched what is being called Operation: Payback. Operation: Payback had previously been directed against the websites of law firms that pursued online music pirates, as well as against the Recording Industry Association of America (RIAA) (Leigh, 2011, p. 207). Because of the WikiLeaks phenomena, today thousands of protesters and sympathizers

---

[20] *Distributed denial-of-service (DDoS) attack prevents a website or other network resources from being available to users (an attacker attempts to prevent legitimate users from accessing information or services) (http://www.us-cert.gov/cas/tips/ST04-015.html).*

[21] *'Amazon subsequently received a call from a staff member of the Homeland Security and Government Affairs Committee on the same day, who questioned the company about their relationship with WikiLeaks. Immediately after the call, Amazon decided to terminate their hosting duties to WikiLeaks' (Arthur, 2010).*

[22] *Wikileaks is a non-profit organization that depends on donations.*

[23] *WikiLeaks currently continues to operate with number of mirror sites (http://mirror.wikileaks.info/), if and when the main (www.wikileaks.org) site is down.*

around the world have joined a virtual internet gathering under Anonymous group. Anonymous also uses a typical web-attack strategy[24] - distributed denial-of-service (DDoS) and has targeted several websites: *Paypal, Mastercard, Visa, Amazon, the PostFinance site* and *the Swedish Prosecution Authority* (Walker, 2010). In the public statement, the Anonymous said: "ongoing attacks were a 'symbolic action' targeted at corporate website that had withdrawn services from WikiLeaks" (BBC, 2010). They also hit the websites of the politicians Sarah Palin and Senator Joe Lieberman, who are among WikiLeaks' loudest critics, and the Swedish prosecutor and lawyers involved in pressing for Julian Assange's extradition from London" (The Economist, 2010).

According to Hardy (2011, p. 157) Operation: Payback and the cyber-attacks launched by the Anonymous "were designed to intimidate governments and organisations into changing their policies on censorship, piracy and confidentiality issues."

AnonOps Communications: The New Strategy

Following a different agenda, today WikiLeaks is trying to spread the information from WikiLeaks' secret diplomatic cables and other leaked material in as many ways as possible. The new 'tactic' is called Crowdleak (previous project Operation: Leakspin) and the idea of the project is to release details from the leaked cables that the mainstream media had overlooked, summarise them "into chunks that everyone can understand" and post it in innocuous locations, as in YouTube videos, social networking websites and on message boards (BBC, 2010). In order to achieve this goal, they allow anyone to volunteer to help them by writing and translating articles, fact checking, editing articles and finally making sure the website remains active and popular (Crowdleaks, 2011).

Based on the facts and information, as well as previous and current events linked to WikiLeaks we can agree with Micah Sifry saying *"age of transparency is here. Not because one transnational online network dedicated to open information and whistle-blowing named WikiLeaks exists, but because the knowledge of how to build and maintain such networks is now widespread. WikiLeaks is just one piece of a much larger continuum of changes in how the people and the powerful relate to each other in this new time changes that are fundamentally healthy for the growth and strength of an open society. Secrecy and the hoarding of information are ending; openness and the sharing of information are coming."* (*http://www.huffingtonpost.com/micah-sifry/wikileaks-assange-micah-sifry_b_820671.html, 6 June 2011).*

[24] *In January 2011, after Anonymous being accused of hacking many websites, they explained in the open letter to the UK government, what is the difference between a DDoS attack and hacking: »hacking as such is defined by the law as 'unauthorised access to a computer or network', whereas a DDoS attack is simply a case of thousands of people making legitimate connections to a publicly accessible webserver at the same time, using up the entire bandwidth or processing power of the given server at once and thereby causing a huge 'traffic jam'.«*

Conclusion

Throughout the 40 years of existence and expansion of ICT, security relevance of cyberspace has changed dramatically, both, nationally and globally, just as the societies have. Certainly, one of the decisive factors causing this was the commercialisation of the information technology and its expansion beyond the national security system. This has also been proved by an analysis of basic concepts which saw cyberspace, both, as a threat and a comparable advantage. At first, they were derived from a defence and military area and saw ICT mainly as a technology which will alter the perception of reality (from the point of view of intelligence), increase the preciseness of conventional weapons beyond imagination as well as establish a decentralised command and control system which will function even in the most impossible of situations. The more the number of civilians increased, the more the concepts were emphasising the part of information warfare, which is to be based on similar grounds as publicity and psychological operations. In light of global geostrategic changes, the 1990s represented the peak of ideas on information warfare, the more radical ones even presuming the conflicts to completely move from a realistic space into a virtual one. Of course, this has not happened. What is more, state structures acquired a completely equal "co-speaker" within cyberspace, both, in form of technically competent individuals and international associations. The aim of the present paper was to focus especially on the latter ones. Although it has been assumed for a long time that, especially in the field of politics and security, there was a strict separation line between the developments in the cyberspace and those in reality, this line was slowly crossed by expanding the services based on the second-generation web. At first, the users, of course, had to be motivated to convert from passive readers into active ones, who would also produce such information. In the first phase, the services, such as YouTube, Wiki, file exchange and sharing portals and, last but not least, social networks, thus had to satisfy the users' need for entertainment, before becoming the backbone of global communication. From a state's point of view, the ghost has left the bottle, intentionally or not. Today, it is therefore impossible to maintain a high level of confidentiality and privacy, which is, all in all, also proven by different Slovenian examples ranging from Udba.net to the Mikstone1 blog. The tendencies for perfect transparency (which surprisingly stopped at publishing information on the functioning of authorities in western countries) have undoubtedly culminated in the WikiLeaks movement with its publishing, but mainly accumulation of data and their decentralised storing. This aspect is important mainly from a political and morally ethical point of view, while, from a security point of view, lateral developments may appear even more important. Cyber battles between the supporters and opponents of the project have also affected parts of critical infrastructure. Of course, in the end, we should mention the responses which have been rather radical, particularly at state levels. In the USA, even students have been warned that browsing through and spreading WikiLeaks data may affect their chances of employment in the national security sector. Numerous ideas have emerged on how to put norms on cyberspace and operations within it, both, at national level as well as internationally (UN). It is an undisputable fact that dealing with cyberspace from a security point of view no longer implies warning against potential future misuse, because it has already become a reality. Centres of social power have changed accordingly,

the most important ones including the platforms and services called Web 2.0. While, throughout human history, physical communication has been subjected to geostrategic efforts, the 21st century made a decisive emphasis on the control of digital communications, both physically and with regard to services. Commercial actors and certain individuals as well as nation states and international organisations dealing with collective defence and security are all well aware of this fact. There is only one question arising thereof – will we enter a new Cold War, which could also take place in the relation state-citizen or in the fight against everybody within cyberspace, or such use of ICT will prevail, which will reinforce positive peace, dialogue, cooperation and solidarity.

Bibliography

1. *Arquilla, J., Ronfeldt, D.,1999. The Advent of Netwar: Analytic Background. Studies in Conflict and Terrorism 22 (3), pp. 193-206.*
2. *Arthur, Charles, 2010. WikiLeaks under attack: the definitive timeline. http://www.guardian.co.uk/media/2010/dec/07/wikileaks-under-attack-definitive-timeline, 1 June 2011.*
3. *BBC, 2010. US embassy cables: The background. http://www.bbc.co.uk/news/world-us-canada-11862320, 4 June 2011.*
4. *BBC, 2010. UK Government websites may be next pro-Wikileaks focus. http://www.bbc.co.uk/news/technology-11990288, 3 June 2011.*
5. *Bilgin, P., 2003. Individual and Societal Dimensions of Security. International Studies Review 5 (2), pp. 203-222.*
6. *CASAGRAS, an EU Framework 7 Project, 2009. http://www.rfidglobal.eu/userfiles/documents/CASAGRAS26022009.pdf, 2 June 2011. .*
7. *Chertoff, M., 2008. The cyber security challenge. Regulation & Governance (2008) 2, pp. 480-484.*
8. *Crowdleaks, 2011. Official website: http://crowdleaks.org/, 4 June 2001.*
9. *Davies, J. G., 2011. From Crowdsourcing to Crowdservicing. Internet Computing 15(3), pp. 92-94.*
10. *Deibert R. J. in Rohozinski R., 2010a. Risking Security: Policies and Paradoxes of Cyberspace Security. International Political Sociology 2010 (4), pp. 15-32.*
11. *Deibert R. J. in Rohozinski R., 2010b. Liberation vs. Control in Cyberspace. Journal of Democracy 21(4), pp. 43-57.*
12. *Denning, D. E.,1999. Information Warfare and Security. Indianapolis: Addison-Wesley.*
13. *Der Derian, J., 2000. Virtuous war/virtual theory. International Affairs 76(4), pp. 771-778.*
14. *Ebersbach, Anja, Glaser Markus, Heigl Richard, Warta Alexander, 2008. Wiki: Web Collaboration: Berlin, Heidelberg: Springer.*
15. *Evropski ekonomsko-socialni odbor: TEN/436 Nova" uredba o Evropski agenciji za varnost omrežij in informacij. Mnenje Evropskega ekonomsko-socialnega odbora o predlogu uredbe Evropskega parlamenta in Sveta o Evropski agenciji za varnost omrežij in informacij (ENISA), 2011.*
16. *Fenster, Mark, 2011. Disclosure's Effects: WikiLeaks and Transparency. Florida: Levin College of Law.*
17. *Fogarty, Jim, 2010. Wikileaks, transparency, and national security: A website that exposes secrets has raised the ire if the U.S. government. New York: The Epoch Times, p. 5. http://epoch-archive.com/a1/en/ca/yeg/2010/06-Jun/17/Page%2005%20World.pdf, 31 May 2011.*

18. *Geers, K.,2009. The Cyber Threat to National Critical Infrastructures: Beyond Theory. Information Security Journal: A Global Perspective 18, pp. 1-7.*
19. *Geers, K.,2010 (a). The challenge of cyber attack deterrence. Computer law & security review 26 (2010), pp. 298-303.*
20. *Geers, K.,2010 (b). Cyber Weapons Convention. Computer law & security review 26 (2010), pp. 547-551.*
21. *Hardy, Keiran, 2011. WWWMDs: Cyber-attacks against infrastructure in domestic anti-terror laws. Computer Law & Security Review. 27-2, pp. 152-161.*
22. *Harknett R. J. in Stever J. A., 2011. The New Policy World of Cybersecurity. Public Administration Review • May | June 2011, pp. 455-460.*
23. *http://arpanet.co.tv/, 20 May 2011.*
24. *http://www.huffingtonpost.com/micah-sifry/wikileaks-assange-micah-sifry_b_820671.html, 6 June 2011.*
25. *http://www.jgzumwalt.com/index.php/articles/251-assessing-wikileaks-damage-to-us-national-security, 30 May 2011.*
26. *http://www.techpluto.com/web-20-services/, 28 May 2011.*
27. *http://www.wired.com/science/discoveries/news/2009/03/dayintech_0317, 25 May 2011.*
28. *Hughes. R., 2010. A treaty for cyberspace. International Affairs 86: 2 (2010), pp. 523-541.*
29. *In the Crossfire Critical Infrastructure in the Age of Cyber War, 2009. http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf, 2 June 2011.*
30. *Kämmerling, Andi, 2011. What is behind Wikileaks? Domo Ringier AG, Corporate Communications, March 2011, p. 10-13. http://domo.ringier.com/wp-content/uploads/2011/03/DOMO_2011m03_en1. pdf, 31 May 2011.*
31. *Khatchadourian, Raffi, 2010. No Secrets: Julian Assange's mission for total transparency. The New Yorker: http://www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian, 1 June 2011.*
32. *Klimburg, A., 2011. Mobilising Cyber Power. Survival 53(1), pp. 41-60.*
33. *Kling, R., 2000. Learning About Information Technologies and Social Change: The Contribution of Social Informatics. The Information Society 16(3), pp. 217-232.*
34. *Leight, David and Harding Luke, 2011. WikiLeaks: Inside Julian Assange's War on Secrecy. London: Guardian Books.*
35. *Liotta, P. H., 2002. Boomerang Effect: The Convergence of National and Human Security. Security Dialogue (33) 4, pp. 473-488.*
36. *Malešič, M., 2004. Environmental security; a case of Slovenia. In: Mahutova, Katarina - Barich, John J., Kreiznebeck, Ronald A. (eds.). Defense and the environment: effective scientific communication, (NATO science series. Series IV, Earth and environmental sciences, vol. 39). Dordrecht; Boston; London: Kluwer Academic Publishers, pp. 139-152.*
37. *Michael, J. B., Tikk, E., Wahlgren, P., Wingfield, T. C. (2010). From Chaos to Collective Defense. Computer 43 (8), pp. 91-94.*
38. *Munro, I., 2009. Defending the Network Organization: An Analysis of Information Warfare with Reference to Heidegger. http://org.sagepub.com/content/17/2/199.*
39. *Myrli, S., 2011. NATO and Cyber Defence. Military Technology 2011(3), pp. 86-90.*
40. *Nissenbaum, H., 2005. Where computer security meets national security. Ethics and Information Technology (2005) 7, pp. 61-73.*
41. *Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV-1), p. 3677. Uradni list RS, št. 27/2010 z dne 2. 4. 2010.*

42. *Saydiari S., 2004. Cyber defense: art to science. Communications of the ACM 47 (3), pp. 53-57.*
43. *Steller, C., 2009. What is Wikileaks? http://minnesotaindependent.com/28719/what-is-wikileaks, 2 June 2011.*
44. *Sund, C., 2007. Towards an international road-map for cybersecurity, Online Information Review 31(5), pp. 566-582.*
45. *Svete, U., 2005. Varnost v informacijski družbi. Ljubljana: Fakulteta za družbene vede.*
46. *Škrubej, J., 2008. Hladna vojna in bitka za informacijsko tehnologijo. Ljubljana: Pasadena.*
47. *The Economist, 2010. The 24-hour Athenian democracy. http://www.economist.com/blogs/babbage/2010/12/more_wikileaks, 3 June 2011.*
48. *The Economist, 2010. The war on WikiLeaks: Sound, fury but few results so far as America tries to fight back against WikiLeaks. http://www.economist.com/node/17674107, 2 June 2011.*
49. *US Pentagon to treat cyber-attacks as ‚acts of war', 2011. http://www.bbc.co.uk/news/world-us-canada-13614125, 2 June 2011.*
50. *W32.Stuxnet Dossier, 2011. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, 2 June 2011.*
51. *Walker, R. Chrisopher, 2010. A brief history of Operation Payback. http://www.salon.com/news/feature/2010/12/09/0, 3 June 2011.*
52. *Walt, S. M.,1998. One world, many theories. Foreign Policy (Spring 1998), pp. 29-35.*
53. *Waltz, K. N., 2000. Structural Realism after the Cold War. International Security 25 (1), pp. 5-41.*
54. *WikiLeaks, 2011. Official website: www.wikileaks.org, 30 May 2011.*
55. *Zumwalt G., James, 2010: Assessing WikiLeak's Damage To U.S. National Security. Human Events, p. 12.*