WAS STUXNET AN ACT OF WAR?

JÂNIS JANSONS

ABSTRACT

Modern societies live in the complex and fragile information environment, in which data processing and exchange grow exponentially. Different digital computerized systems support most of key infrastructures like financial systems, power and water supplies, air traffic management, public and military communications. To increase accessibility to those systems in the information domain, it requires interoperability and interconnectivity which makes them complex to maintain and vulnerable to cyber-attacks/intrusions. The Internet is an ownerless, ubiquitous and open to all information exchange domains which can shape the international relations through the cyber domain and there is no international entity that can control and affect the data flow. Each country has its own legislation to react and influence local users through Internet service providers and only close cooperation among the states can help to identify and prevent illegal activities against other states as well as support foreign countries during investigations. The paper will uncover how cyber weapon was used to influence state struggling, becoming a nuclear power for the first time. It is divided into two parts to explain the essence of the act of war and cyberspace to understand the environment where Stuxnet was applied. Next it will focus on impact and reaction of Stuxnet in order to analyse its utilization within cyberspace.

KEY WORDS

Cybersecurity, Internet, Stuxnet, act of war.

DOI: 10.26410/SF_1/17/11

JÂNIS JANSONS[1]

janis.jansons@stud.baltdefcol.org

Baltic Defence College,

Tartu, Estonia

[1] Opinions expressed by the author are his own views and they do not reflect in any way the official policy or position of the Baltic Defence College, or the governments of Estonia, Latvia or Lithuania.

Introduction

Modern society lives in the complex and fragile information environment in which data processing and exchange grow exponentially. Different digital computerized systems support most of key infrastructures like financial systems, power and water supplies, air traffic management, public and military communications. To increase accessibility to those systems in the information domain, it requires interoperability and interconnectivity which makes them complex to maintain and vulnerable to cyber attacks/intrusions. Furthermore, this new reality of information exchange shows that societies highly depend on information and communication technologies, which

are interconnected in one global network named the Internet. This addiction to the Internet is a major source of vulnerability and full control over the information domain in these conditions is almost impossible. So, somebody could use those vulnerabilities to breach national security and influence an economic, political and social situation in other countries.

The Internet is an ownerless, ubiquitous and open to all information exchange domains, which can shape the international relations through the cyber field. The Internet is a computer network that uses standardized protocols to interconnect states, organizations and individuals worldwide. Neither states nor organizations, nor single persons are the owners of the Internet. While there is one non-profit organization which simply manages Internet protocol numbers and the Domain Name System root, and the others provide a piece of infrastructure just to be part of the Internet. There is no international entity that can control and affect the data flow. Each country has its own legislation to react and influence local users through Internet service providers. Only close cooperation among the states can help to identify and prevent illegal activities against other states as well as support foreign countries during investigations. So, the states' political willingness to cooperate in the cyberspace shapes dialogue internationally. However, there are some fuzzy cases where some cyber activities originating in one state that are against another state critical infrastructure could be interpreted as an act of war or a covert action.

This paper will uncover how cyber weapon was used to influence state struggling, becoming a nuclear power for the first time. Was the use of cyber weapon an act of war? This paper will claim that Stuxnet was not an act of war, but rather a covert action with possible future consequences. To argue this statement, this paper is divided into two parts, where the first part will explain the essence of two terms – an act of war and cyberspace to understand the environment where Stuxnet was applied. The second part will focus more on an impact and reaction of Stuxnet in order to determine it.

An act of war and cyberspace

The phrase 'Act of war' is characterised as a political term rather than a military or legal one (Nakashima E., 2012). This term is used in an international environment by politicians in situations where it was a violent and non-violent act. Terrorist attacks (Cella M., 2015), key leader killings (Strange H., 2013), shooting down airplane during peace time (Vinogradov D., 2015), the blockade of sea lines of communication (Global Research, 2015), imposing economic sanctions (Saundersaug P.J., 2014), cyber-attack (Gorman S., and Barnes E.J., 2011) etc., have motivated politicians to use the phrase 'an act of war'. This term does not have a standard definition worldwide and its application to cyber incidence seems to be questionable. However, there is a country which defines them as 'acts of war'. For example, the United States (U.S.) to prevent possible cyber Pearl Harbor (Stiennon, R., 2015) came to the conclusion that cyber-attacks originating from another country can be interpreted as an 'act of war' to counter using all kinds of military force (Gorman S., and Barnes E.J., 2011). However, the international law avoids the term 'an act of war' in favour of other phrases like 'illegal intervention', 'the use of force', 'armed attack', or 'an act of aggression'. For example, an act of aggression includes more serious uses of force and armed attack, whereas all uses of force are not only

armed attacks, but could also be illegal interventions (Fidler D.P., 2011). Despite those definitions, legal experts Charles Dunlap, a retired Air Force Major General and professor at Duke University law school, or retired Gen. James Cartwright, former vice chairman of the Joint Chiefs of Staff argue that only the president and Congress in the U.S. could decide that the social or financial impairment is sufficient to consider a cyber-attack as an act of war (Nakashima E., 2011). So, the use of this term depends on the leaders of the targeted country, who would decide whether or not to respond with military force to cyber-attacks. As a result, the phrase 'an act of war' becomes more political. If it is so, then what could be the trigger for politicians in cyberspace to respond militarily? For this reason, it is important to understand cyberspace.

Cyberspace, like the term 'act of war' has no single internationally recognised definition. Cyberspace is a revolutionary human-made, ubiquitous, networked, and virtual environment which seems to be driven by swift electronic communication and progress in information technology. This is a possible way of explaining cyberspace in own words. In spite of this innovative sketch, the overall definitions of cyberspace are disputable (Ottis and Lorents, 2010). Therefore, trying to find an exact, perfectly expressed definition of cyberspace seems to be impossible. It is therefore more prudent to stick to one definition and to analyse step-by-step what these separate components are.

Firstly, it is important to examine some historical background of wording, which could be the main milestone of further definitions. The term cyber appears to be the Greek word *kybernetes*, which means steersman or the governor. So, in 1948, to appreciate the Maxwell control loop feedback mechanism, the famous mathematician and philosopher Wiener (1985) introduced the first application of cyber as 'cybernetic – the entire field of control and communication theory, whether in the machine or in the animal'. In the initial stages of technology development, the term cyber relates originally to data processing and intercommunication activities or it can be called the 'Wiener component' of cyberspace definition. However, in later years, a word cyber was used so to emphasize another environment in networks and computers rather than physical appearance.

Secondly, a prefix cyber is basically exploited as the part of a composite word, then it is used as a single term. A compound word, for instance cyberspace could be considered in order to obtain a metaphysical or meaningful definition. Without knowing about computers and the Internet, a speculative fiction novelist and essayist Gibson (1984) in his novel *Neuromancer* introduced for first time the word cyberspace as 'a consensual hallucination' on the computerized network. That means its appearance provides any kind of physical medium. This could lead to the feeling of outside of physical reality, which is more related to 'Gibson's component' of cyberspace definition. Seamlessly using the advantages of new technologies, human beings tend to believe in the existence of such an environment. This stimulates the search for a comprehensive and coherent definition, where actors are the key element to interact in this environment.

The lack of security in cyberspace offers an opportunity for a wide range of actors like in social -physical space, where persons have various reasons and capabilities to challenge law enforcement. Originally, unauthorized actors in cyberspace were cyber criminals, whose strong intent was to gain financial benefits; blackmailers, who used evidence to intimate key leaders,

or simply hackers, who wanted to prove their brain potential. Moreover, the national government and non-government actors like private institutions, crime and extremist groups, subsidised agents are capable of demonstrating cyber attacks in a more sophisticated way. In the targeted states, those groups of attackers might undermine the financial system, and disrupt the critical infrastructures (Omand, 2013). The actors are divided into two main groups as insiders and outsiders.

Insiders are most harmful to an organization they work for. Insiders are trusted parties such as current and former employees, service providers, and business partners, who have knowledge of the insides and security measures of an organization and access to organization network or even sensitive information. Two examples of insiders who caused serious damage to government organizations are a former soldier of the U.S., Bradley Edward Manning and former Central Intelligence Agency employee Edward Joseph Snowden. Manning was convicted after disclosing sensitive military and diplomatic documents to WikiLeaks, which he, as an intelligence analyst, elicited from classified databases. The second famous insider, Snowden, was able to copy information from the U.S. National Security Agency (NSA) and after then publicly released the sensitive information about numerous global surveillance programs. Both cases carried out by insiders have weakened the national security of the country and relations with various international partners (Sovereign Intelligence, 2014).

Outsiders are a defined group of attackers, who are possible to split into three main groups such as individuals, non-government organizations and government organizations (Geest, 2015).

Individuals as potential cyber attackers could be divided into three main subgroups: amateurs, hackers and hacktivists. Amateurs or beginners can easily learn the first steps for hacking on the internet by doing a certain category of attacks. However, hackers are more capable of threatening any computerized system. This preconception is not always the true description of hackers due to their different attitudes. Hackers are noticeably divided into white (blue), grey and black hat hackers (Kovacs, N., 2015). White and grey hat hackers break the security for testing vulnerabilities to improve computerizes systems. The only difference is that grey hat hackers target the system without the owner's authorization or awareness. They inform the system administrator about the discoveries and sometimes ask for a fee to resolve security problems. Although this attitude of hackers appears to be ethical, the unauthorized access is illegal. A black hat hacker is cybercriminal, who uses his abilities only for malicious or unlawful purposes to gain financial profit (Graves, K., 2010).

Non-government cyber organizations are mostly cybercriminal and ideological groups like anonymous cyber protesters. A hacktivist or anonymous cyber protester is predominantly driven by a political reason rather than financial benefits. They are able to build virtual groups, which conduct an amount of cyberattacks to fight the state powers and large industries when they step over the "red" line. In 2014, before the release of the comedy *The Interview* on the fictional assassination of North Korea's leader, an allegedly hacktivist group attacked Sony Pictures Entertainment leaking company's classified information. The U.S. government, however, suspects that North Korea government sponsored the hacker group and is behind these attacks and as a consequence, this issue escalated into a diplomatic crisis between two countries (Grisham, L., 2015). So, those

cyber incidences possibly by hacktivists were able to raise public attention and diplomatic consequence without gaining any financial benefit. However, organized criminal groups make profits and disappear before law enforcement identifies them (Broadhurst, R., etc., 2014). Global cybercriminal organizations exist and have structures similar to the Mafia (Peachey, P., 2014), some of them are protected by weak and corrupted governments (Rifkind, J., 2011). Criminal organizations make profits by buying and selling stolen individual's bank credit cards information and company's intellectual properties. Conversely, ideological groups have more extensive goals, which occasionally are politically motivated and supported by government organizations to keep within an international law (Garcia E.C., 2010).

Government organizations or nation-states have largest capabilities and they can target a wide array of institutions and individuals from private and government research and development institutions to defence, finance and public sector organizations. Government-organized attacks could range from the dissemination of propaganda to intelligence gathering to multiform operations on critical infrastructures, for example Russian online "troll" (Iasiello, E., 2015), 'Titan Rain' operation, and 'Olympic Games' Operation (Stiennon, R., 2015. p. 125).

The main effort of cyber attacks is to gain economic benefits rather than political or military dominance. Organized cyber attacks actively disrupt the information and communication systems of the financial institutions, and cause serious reputation and economic damage. Reputation damage is more related to the company, trust and ability to safeguard costumers' and own money. In order to reduce probable direct financial loss and to recover expenditures from cyber attacks, companies and governmental institutions need to provide the additional cost of securing networks. Global cyber activities profit yearly up to US$1 trillion, which are comparatively more than global drug trafficking and piracy together (McAfee, 2013). That means overall cyber activities focus more on a finance sector rather than on overcoming the security systems of the well protected governmental information and communication system. The illegal money is very attractive for people and government services cannot offer big enough salary to discourage skilled hackers to be out of illegal sector. This requires respective resources and an organized structure, which is capable of producing sophisticated cyber tools to penetrate the well protected system or even standalone systems.

Cyber attacks are a major influence tool during or before major political and military conflicts. Traditional dominant cyber actors in the international arena are the USA, Russia and China, all of which have huge capabilities and resources to support cyber offensive operations (Lewis J., 2013). For example, Russia dominates the neighbouring countries in the cyber space. In 2007 the Estonian government decided to relocate the Soviet time memorial from the centre of a capital city to a military cemetery. Putin's supported regime shamed Estonians and reacted to the relocation with the cyber power. Estonia suffered widespread politically motivated cyber attacks that were first brute-force denial of service attacks from Russia. This cyber incident lasted several days and paralyzed the information domain of Estonia, an electronic banking system and affected the daily life of Estonian citizens (Traynor I., 2007). However, this cyber attack was not declared as an act of war. So, in 2007 Estonia did not use NATO Article 5. However, during Georgia War in

2008 and Ukraine crisis in 2013 real Russian tactics was disclosed, and cyber tools were used in tandem with a conventional military campaign. In the Georgia War the Russian state hired companies like Rostelecom and Comstar and volunteer cyber warriors were blocking the internet traffic in Georgia. Moreover, in 2014 attackers from Russia targeted a computerized election system in Ukraine to disrupt presidential election results from around the country. Before this cyber-attack the government officials and security units of Ukrainian battling pro-Russian rebels were targeted to cripple intelligence-gathering and decision-making (Coker M., and Sonne P., 2015). In those cases there was no evidence that Russia as a state was certainly behind the attacks (Kirchner S., 2009). These facts indicate that government sponsored them and covert cyber attack tend to be more sophisticate and capable of achieving political and military goals. Despite this fact, another political engagement seems to be used during the 'Olympic Games' Operation.

The Stuxnet worm

The 'Olympic Games' Operation was a secret campaign under which Stuxnet worm was formed (Stiennon, R., 2015). Some provided thoughts that Stuxnet could be a starting point in a new era of cyber war. Some higher education institutions claim that a cyber war is the highest level of cyber conflict between or among states in which actors acting on behalf of a governmental body carry out cyber attacks as part of military operations (Godwin J.B., et al 2014). Based on the empirical definition, war is possible between states if the conflict involves at least 1,000 battle-related deaths per year (Harrison L., et al 2015). Rid convincingly argued that Stuxnet was not connected to a conventional military operation and did not kill any military person (Rid T., 2013). Some argued that Stuxnet was the first demonstration of a cyber offensive capability which is able to carry out physical destruction of strategic targets in military style (Broad W.J., et al 2011). Fidler was also not certain to define the Stuxnet release as an act of war (Fidler, D.P., 2011). Former head of the NSA[1] and CIA[2] director, retired general Hayden fully rejected a view that Stuxnet was an act of war (CBSNews., 2012). However, it is clear that the Olympic Game Operation is still officially not acknowledged military campaign. For that reason, there are so many denials, many rumours and uncertainty around Stuxnet. To prove Hayden and reject Fidler argument, it is necessary to understand what Stuxnet and its impact on target was, and what reactions to this cyber incident were.

The goal of Stuxnet was to destroy or significantly delay Iran's potential nuclear weapon production capability. The main focus was a Natanz uranium enrichment plant where there were thousands of centrifuges used to enrich the uranium gas. The worm was able to shut down and cause damage to 984 centrifuges that spin uranium gas material (Albright D., et al 2010). After this attack Iran ceased work at its nuclear facilities without explanation to international community (Katz Y., 2010). It is unclear that the worm was the reason to do so.

Stuxnet has more technical sophistication and precisely targeted malware than a normal computer worm. A worm is a code which is capable of running without host program, self-reproducing and spreading

[1] National Security Agency – an intelligence organization of the United States government, responsible for global monitoring, collection, and processing of information and data for foreign intelligence.

[2] Central Intelligence Agency – a civilian foreign intelligence service of the U.S. Government, dealing with gathering, processing and analysing national security information from around the world, primarily through the use of human intelligence.

to other computer systems through downloaded files or network. The worm can spread using one or more methods like email, instant messaging and file-sharing programs, social networking sites, network shares, removable drives with Autorun enabled, and software vulnerabilities (Microsoft, 2015). In 2010 Stuxnet was discovered in the databanks of critical infrastructures like power plants, traffic control systems, and different factories around the world (Keizer G., 2010), but Iran was the most targeted country with about 60% of all infection (Halliday J., 2010). Stuxnet was able to manipulate the speed of centrifuges and damage the uranium enrichment process. At the same time this worm was changing Siemens SCADA[3] control software parameters in such way that system's indicators show normal working condition (Langner R., 2013). Unlike most worms. Stuxnet does not use the usual forged digital certificates that help to intrude into computer systems. It actually used real stolen Realtek Semiconductor and JMicron Technology Corporations, global microchip producers in Taiwan, digital certificates which allow intruders to sign fake software drivers for Windows operating systems (Zetter K., 2011). Stuxnet exploited security holes in the systems. Those gaps that system creators are unaware of are known as zero-day vulnerabilities. The details of zero-day vulnerabilities are extremely valuable and can be sold on the black market for five to several hundred thousand U.S. dollars each (Zetter K., 2014). The most successful malwares use them and Stuxnet was not exceptional. Actually, Stuxnet used 20 zero-day vulnerabilities (Rapoza K., 2012) to penetrate a computer system. When accessing the system, this worm does not always activate. In Stuxnet codes specific Siemens settings of programmable logic controllers (PLC) were defined that control and monitor the speed of the centrifuges (McMillan R., 2010). It was searching for this specific target and without that target, the worm remains hidden (McMillan R., 2010).

It is unclear if Stuxnet was effective to reach political goals, but it was the motivation for Iran to develop cyber capabilities. Iran increased its cyberwarfare capabilities with different organizations like the High Council of Cyberspace, Cyber Defence Command, loyal, high skilled hacker group named Iranian Cyber Army, which has links with the Revolutionary Guard and the Asiana hacker forum (Wheeler A., 2013). The Iranian Cyber Army was behind a wave of cyberattacks on the U.S. banking systems, and they hacked into Israeli computers to steal information from government officials (Baker J.W., 2015.). So the Iranians seem to have or try to find evidence which countries were involved to build and release Stuxnet.

Only a state or group of states seems to be willing and able to build and use such cyber weapon like Stuxnet. The major issue for the United Nations (UN) was to prevent Iran from getting the nuclear bomb. In 2006 the UN Security Council's (UNSC) five permanent members; namely China, France, Russia, the United Kingdom (UK), and the USA; plus Germany struggled with diplomatic efforts to stop the Iranian nuclear program without success (Küntzel M., 2015). Moreover, in 2008 UNSC adopted new Resolution 1803 to enforce all steps from the previous resolution. In 2009 the USA started shaping world community attention against Iran, and Israel threatened with possible nuclear action (Lyons K., 2015). It was unclear if a U.S. conventional attack would stop the Iranian nuclear program. Beside that it could induce Middle East in another war and the Americans would not be ready for uninterrupted military actions and possible growing oil price (Blas

[3] Supervisory Control And Data Acquisition.

J., 2012). It appears that the USA and Israel were searching for desired outcome with minimal effort and maximum gains. There is no sufficient and conclusive evidence beyond rumours which country could have the potential to develop such cyber weapon and be willing to attack Iran in 2010. However, only an economically developed country could afford at least 400$ million to develop the Stuxnet worm (Langner R., 2010), because according to the previous argument, individuals or organized criminals are more interested in gaining money rather than in spending it. Due to this fact, some argue that the USA was involved in the testing and development of expensive cyber weapons. Others believe that Israel is responsible for the attack, because the worm code has the biblical reference (Timmerman K., 2010). Iran's officials accused Siemens Mobile Company, whose software was used to prepare the ground for the Stuxnet worm (The Telegraph 2011). There is some evidence, but not a real investigation and lack of state cooperation to find out who was behind Stuxnet. If there is no clear proof about the involvement of a state and conventional military troops, there is no reason for defining Stuxnet as an act of war.

Stuxnet does not have a warlike nature to influence a political and military condition of another state. According to Clausewitzian's concept of war as a continuation of politics by other means, Rid argued that any act of war related to cyber incidents has to be lethal, has to have clear means and ends, and has to be politically motivated or the state should be behind them (Rid T., 2013). The Stuxnet worm had clear means and ends to significantly affect the Iranian nuclear program. Moreover, anonymous sources indicated that at least two states were involved in launching the operation. Despite those facts, Stuxnet did not result in any battle deaths of military personnel. Although it seems to be a new form of war, which skips the battlefield, by definition any war should be violent. That means this cyber attack has not warlike nature, but it could be a kind of a hidden action performed by a state to influence the opponent state.

The Stuxnet worm is most likely a covert action supported by the U.S. Government. Mr. Sanger's book was published in 2012 and it brought a fast request from an American Republican party to investigate by the FBI the leaks of information about a U.S. covert cyber operation to shut down Iran's nuclear enrichment facilities with a computer worm named Stuxnet (Scarborough R., 2013). According to Mr. Sanger information *"Should we shut this thing down?" Mr. Obama asked, according to members of the president's national security team who were in the room"* it seems to be secretly ordered by the U.S. president to use Stuxnet in order to delay the Iranian nuclear program. Based on the domestic legal framework, the president has two possibilities to authorize a cyber attack against another state. So, the Olympic Game operation should rely on military or intelligence legal authority. Under the military domain, it could be difficult to carry out cyber attacks without triggering solid diplomatic and security problems for the USA, but the intelligence domain has more flexibility to maintain hidden cyber attacks (Brecher A.P., 2012). According to National Security Act Sec. 503 (e), the U.S. Intelligence community has the possibility to clandestinely prepare personnel who is not uniformed military personnel to attack an enemy. The U.S. policymaker defined this activity as a covert action *"to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly"*

(Peritz A.J., Rosenbach E., 2009). Moreover, during an interview about Stuxnet, the former head of the National Security and CIA director Michael Hayden said that this cyber attack was not a warlike activity because the opposite site did not respond as if it was an act of war. He is sure that this cyber incident was a thing between peace and war, so called a covert action (CBSNews, 2012). Thus, it could be the reason why there are only rumours and no investigation to find out which country is behind the Stuxnet worm.

Conclusion

To conclude the findings of this essay, the phrase 'an act of war' is political rather than a legal term because the international law uses different terms and a country which defined it needs to have its political leadership decision to respond with military force to the attacks in cyberspace. Cyberspace is a complex and dynamic environment which is characterised by two components – physical (Wiener) and non-physical (Gibson), where actors are the part of the physical element. The lack of security in cyberspace offers an opportunity for a wide range of actors who have various reasons and capabilities to challenge law enforcement. The predominance of cyber attacks effort seeks to gain economic benefits. To penetrate the well protected system or even standalone systems, cyber attackers take advantage of the vulnerabilities of information systems and personal information. Therefore, social media is one of the sources where a cyber actor like governmental organizations can use to collate information, and use it in future to break security walls of the system targeting an opponent and, for example, its critical infrastructure. Cyber attacks possibly by the Russian regime against opponent's critical infrastructure are a major influence tool during or before major diplomatic and political trouble or even military conflicts. Russia as a state did not reveal their involvement in those attacks. Due to the complexity of cyberspace and lack of willingness and cooperation to investigate the cyber incident, it is not easy to prove that a state actor was behind the cyber attack.

The Olympic Games Operation under which the Stuxnet worm was possibly formed seems to be another good example of a state sponsoring a secret campaign in the cyberspace. Stuxnet opened a new era of cyber reality by showing a more technically sophisticated and precise approach to destroy or significantly delay Iran's potential nuclear weapon production capability. Since 2006 only some UNSC permanent members like China, France, the United Kingdom (UK), and the USA have been struggling with diplomatic efforts to stop the Iranian nuclear program without success. Therefore, there are many rumours that the USA was involved in the testing and development of expensive first cyber weapon like Stuxnet. Due to lack of clear evidence about the involvement of a state and conventional military troops, there is no reason for defining Stuxnet as an act of war. Beside that Stuxnet does not have a warlike nature because of no battle deaths of military personnel and no willingness of the targeted state to respond. To summarise, the Stuxnet worm is most likely a covert action supported by the state which has offensive cyber capabilities to maintain such an expensive campaign to prevent a possible conventional military attack. Nevertheless, Iranians seem to try to find evidence which countries were behind Stuxnet and seek to retaliate.

Cyber environment is a unique opportunity for cyber powers to shape international relations. Stuxnet has shown a new cyber reality which warned about an impending

'cyber Pearl Harbor'. Therefore, based on those findings in this paper, future political leaders should be aware of the potential of cyber powers, but military leaders should be ready to operate in the complex and fragile information environment in the similar way as it is required in other domains.

References

Albright D., Brannan P., and Walrond C., 2010, Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment (online) Available at http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ (accessed 07.02.2016).

Baker J.W., 2015, Iran: The Cyber Nation – Timeline of Every Hack. (online) Available at http://xpatnation.com/iran-the-cyber-nation-timeline-of-every-hack/#.y77h98T7y (accessed 10.02.2016).

Blas J., 2012, The oil price reaction to an Iranian strike. (online) Available at http://www.ft.com/intl/cms/s/0/e977f55c-f780-11e1-ba54-00144feabdc0.html#axzz41DLBucjD (accessed 12.02.2016).

BNN, 2014, SP: Kremlin-financed internet trolls operate in Latvia (online) Available at http://bnn-news.com/sp-kremlin-financed-internet-trolls-operate-latvia-122404 (accessed 25.11.2015).

Brecher A.P., 2012, Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations. (online) Available at http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1081&context=mlr (accesse d 01.03.2016).

Broad W.J., Markoff J., and Sanger D.E., 2011, Israeli Test on Worm Called Crucial in Iran Nuclear Delay.

Broadhurst, R., etc., 2014, Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. (online) Available at http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf (accessed 08.11.2015).

CBSNews, 2012, Gen. Hayden: Stuxnet virus "Not an act of war". (online) Available at http://www.cbsnews.com/news/gen-hayden-stuxnet-virus-not-an-act-of-war/ (accessed 04.02.2016).

Cella M., 2015, Paris Attacks Called 'Act of War' (online) Available at http://www.usnews.com/news/articles/2015/11/14/paris-terror-attacks-by-isis-called-act-of-war (accessed 11.01.2016).

Coker M., and Sonne P., 2015, Ukraine: Cyberwar's Hottest Front. (online) Available at http://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671 (accessed 25.11.2015).

Fidler, D.P., 2011, Was Stuxnet an Act of War? Decoding a Cyberattack (online) Available at http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5968088&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5968088 (accessed 02.02.2016).

FromDev, 2014, 100+ Free Hacking Tools To Become Powerful Hacker, (online) Available http://www.fromdev.com/2014/09/free-hacking-tools-hacker.html (accessed 06.11.2015).

Garcia E.C., 2010, Regulating Nation-State Cyber Attacks in Counterterrorism Operations. (online) Available at https://www.hsdl.org/?view&did=10513 (accessed 08.11.2015).

Geest, D.S., 2015, Cybersecurity and the dividing nature of global competing ideologies. (online) Available at http://www.hscentre.org/global-governance/cyber-security-dividing-nature-global-competing-ideologies/ (accessed 06.11.2015).

Gibson, W., 1984, Neuromancer. New York: Berkley Publishing Group.

Global Research, 2015, Turkey's Blockade of Russian Naval Vessels' Access to the Mediterranean, Russia's Black Sea Fleet Completely Cut Off. (online) Available at http://www.globalresearch.ca/turkeys-blockade-of-russian-naval-vessels-access-to-the-mediterranean-russias-black-sea-fleet-completely-cut-off/5492688 (accessed 13.02.2016).

Godwin J.B., Kulpin A., Rauscher K.F. and Yaschenko V., 2014, The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, Issue 2. EastWest Institute and the Information Security Institute of Moscow State University.

Goodin D., Puzzle box: The quest to crack the world's most mysterious malware warhead (online) Available at http://arstechnica.com/security/2013/03/the-worlds-most-mysterious-potentially-destructive-malware-is-not-stuxnet/ (accessed 06.02.2016).

Gorman S., and Barnes E.J., 2011, Cyber Combat: Act of War, http://www.wsj.com/articles/SB10001424052702304563104576355623135782718 (accessed 13.02.2016).

Graves, K., 2010, Certified Ethical Hacker study guide. (online) Available at http://ir.nmu.org.ua/bitstream/handle/123456789/133057/768e0fbfd4fe2971f189aecf8c038201.pdf?sequence=1 (accessed 07.11.2015).

Grisham, L., 2015, Timeline: North Korea and the Sony Pictures hack. (online) Available at http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/ (accessed 07.11.2015).

Halliday J., 2010, Stuxnet worm is the 'work of a national government agency' (online) Available at http://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency (accessed 05.02.2016).

Harrison L., Little A., and Lock E., 2015., Politics: The Key Concepts London: Routledge.

Iasiello, E., 2015, Russia's Propaganda Trolls Make an Impact in Cyberspace. (online) Available at http://darkmatters.norsecorp.com/2015/08/27/russias-propaganda-trolls-make-an-impact-in-cyberspace/ (accessed 09.11.2015).

Katz Y., 2010, Stuxnet may have destroyed 1,000 centrifuges at Natanz. (online) Available at http://www.jpost.com/Defense/Stuxnet-may-have-destroyed-1000-centrifuges-at-Natanz (accessed 07.02.2016).

Keizer G., 2010, Why did Stuxnet worm spread? (online) Available at http://www.computerworld.com/article/2516109/security0/why-did-stuxnet-worm-spread-.html (accessed 05.02.2016).

Kirchner S., 2009, Distributed Denial-of-Service Attacks under Public International Law: State Responsibility in Cyberwar. (online) Available at https://www.researchgate.net/publication/251287009_Distributed_Denial-of-Service_Attacks_under_Public_International_Law_State_Responsibility_in_Cyberwar (accessed 15.12.2015).

Kovacs, N., 2015, What is the Difference Between Black, White and Grey Hat Hackers? (online) Available at http://community.norton.com/en/blogs/norton-protection-blog/what-difference-between-black-white-and-grey-hat-hackers (accessed 07.11.2015).

Küntzel M., 2015, Germany and a Nuclear Iran (online) Available at http://jcpa.org/article/germany-and-a-nuclear-iran/ (accessed 12.02.2016).

Langner R., 2010, The short path from cyber missiles to dirty digital bombs. (online) Available at http://www.langner.com/en/2010/12/26/the-short-path-from-cyber-missiles-to-dirty-digital-bombs/ (accessed 14.02.2016).

Langner R., 2013, To Kill a Centrifuge (online) Available at http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf (accessed 05.02.2016).

Lewis J., 2013., Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia (online) Available at http://csis.org/files/publication/130307_cyber_Lowy.pdf (accessed 14.12.2015).

Lyons K., 2015, Iran nuclear talks: timeline (online) Available at http://www.theguardian.com/world/2015/apr/02/iran-nuclear-talks-timeline (accessed 12.02.2016).

McAfee, 2013, The Economic Impact of Cybercrime and Cyber Espionage (online) Available at http://www.mcafee.com/mx/

resources/reports/rp-economic-impact-cybercrime.pdf (accessed 09.11.2015).

McMillan R., 2010, Was Stuxnet Built to Attack Iran's Nuclear Program? (online) Available at http://www.pcworld.com/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html (accessed 06.02.2016).

Microsoft, 2015, Malware Protection Center. (online) Available at https://www.microsoft.com/security/portal/mmpc/shared/glossary.aspx (accessed 15.03.2016).

Nakashima E., 2011, U.S. cyber approach 'too predictable' for one top general. (online) Available at https://www.washingtonpost.com/national/national-security/us-cyber-approach-too-predictable-for-one-top-general/2011/07/14/gIQAYJC6EI_story.html?tid=a_inl (accessed 13.02.2016).

Nakashima E., 2012, When is a cyberattack an act of war? (online) Available at https://www.washingtonpost.com/opinions/when-is-a-cyberattack-an-act-of-war/2012/10/26/02226232-1eb8-11e2-9746-908f727990d8_story.html (accessed 10.01.2016).

Omand, D., 2013, Security Europe: The steps needed to protect the EU's critical infrastructure against cyber-attack. (online) Available at http://europesworld.org/2013/10/01/the-steps-needed-to-protect-the-eus-critical-infrastructure-against-cyber-attack/#.VjzxylLotjo (accessed 06.11.2015).

Ottis, R., Lorents P., 2010, Cyberspace: Definition and Implications. (online) Available at https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf (accessed 02.11.2015).

Peachey, P., 2014, Mafia Cybercrime Booming and With It a Whole Service Industry, Says Study. (online) Available at http://www.independent.co.uk/news/uk/crime/mafia-cybercrime-booming-and-with-it-a-whole-service-industry-says-study-9763447.html (accessed 08.11.2015).

Peritz A.J., Rosenbach E., 2009, Covert Action. (online) Available at http://belfercenter.ksg.harvard.edu/publication/19149/covert_action.html (accessed 01.03.2016).

Rapoza K., 2012, Is It Time For Another Stuxnet Attack On Iran? (online) Available at http://www.forbes.com/sites/kenrapoza/2012/05/28/is-it-time-for-another-stuxnet-attack-on-iran/#1879269474fb (accessed 06.02.2016).

Rid T., 2013, Cyber War Will Not Take Place. London: Hurst.

Rifkind, J., 2011, Cybercrime in Russia. (online) Available at http://csis.org/blog/cybercrime-russia (accessed 08.11.2015).

Rutledge P., 2013, How Obama Won the Social Media Battle in the 2012 Presidential Campaign (online) Available at http://mprcenter.org/blog/2013/01/how-obama-won-the-social-media-battle-in-the-2012-presidential-campaign/ (accessed 25.11.2015).

Sangerjune D.E. Obama Order Sped Up Wave of Cyberattacks Against Iran. (online) Available at http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (accessed 04.03.2016).

Saundersaug P.J., 2014, When Sanctions Lead to War. (online) Available at http://www.nytimes.com/2014/08/22/opinion/when-sanctions-lead-to-war.html?_r=0 (accessed 13.02.2016).

Scarborough R., 2013, In classified cyberwar against Iran, trail of Stuxnet leak leads to White House. (online) Available at http://www.washingtontimes.com/news/2013/aug/18/trail-of-stuxnet-cyberwar-leak-to-author-leads-to-/?page=all (accessed 04.03.2016).

Sovereign Intelligence, 2014, THE INSIDER THREAT: Implications for Corporate Security (online) Available at http://www.sovereign-llc.com/wp-content/uploads/2014/09/SI-Insider-Threat-WP.pdf (accessed 23.11.2015).

Stiennon, R., 2015, There Will be Cyber War: How the Move to Network-Centric War Fighting has set the Stage for Cyberwar. IT-Harvest Press, 2015.

Strange H., 2013, US raid that killed bin Laden was 'an act of war', says Pakistani report (online) Available at http://www.telegraph.co.uk/news/worldnews/asia/pakistan/10169655/US-raid-that-killed-bin-Laden-was-an-act-of-war-says-Pakistani-report.html (accessed 11.01.2016).

The Telegraph 2011, Iran accuses Siemens over Stuxnet cyber-attack. (online) Available at http://www.telegraph.co.uk/technology/news/8457658/Iran-accuses-Siemens-over-Stuxnet-cyber-attack.html (accessed 13.02.2016).

Timmerman K., 2010, Computer Worm Shuts Down Iranian Centrifuge Plant. (online) Available at http://www.newsmax.com/KenTimmerman/iaea-stuxnet-computer-worm/2010/11/29/id/378288/ (accessed 10.02.2016).

Traynor I., 2007, Russia accused of unleashing cyberwar to disable Estonia. (online) Available at http://www.theguardian.com/world/2007/may/17/topstories3.russia (accessed 25.11.2015).

Vinogradov D., 2015, Turkey Committed Act of War By Shooting Russian Plane in Syria. (online) Available at http://sputniknews.com/middleeast/20151124/1030684495/russian-plane-turkey-shot-syria.html (accessed 13.02.2016).

Wheeler A., 2013, The Iranian Cyber Threat. (online) Available at http://phoenixts.com/blog/the-iranian-cyber-threat-part-1-irans-total-cyber-structure/ (accessed 10.02.2016).

Wiener, N., 1985, Cybernetics: Or Control and Communication in the Animal and the Machine. 2nd ed. Cambridge: The M.I.T. Press.

Zetter K., 2011, How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History (online) Available at http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/2/ (accessed 05.02.2016).

Zetter K., 2013, Stuxnet Attack on Iran Was Illegal 'Act of Force' (online) Available at http://www.wired.com/2013/03/stuxnet-act-of-force/ (accessed 10.12.2015).

Zetter K., 2014, Hacker Lexicon: What Is a Zero Day? (online) Available at http://www.wired.com/2014/11/what-is-a-zero-day/ (accessed 06.02.2016).