Acta Informatica Pragensia
3(1), 2014, 23–32, DOI: 10.18267/j.aip.33
Online: aip.vse.cz

Sekce / Section:
Recenzované stati / Peer-reviewed papers

The Third World War? In The Cyberspace. Cyber Warfare in the Middle East.

Martina Knopová[1], Eva Knopová[1]

[1] Institute of Information Studies and Librarianship, Faculty of Arts,
Charles University in Prague
U Kříže 8, 158 00 Praha 5, Czech Republic

martina.knopova@gmail.com

Abstract: This article aims to provide a brief and comprehensive introduction to the issue of cyber warfare and to display the recent development in this area. Geographically, it focuses on the Middle East region, since the vast majority of the most important recent cyber attacks appeared just in there or were connected to it. The first part of the article tries to define the key notion of cyber warfare, compares it to the standard warfare and presents different types of cyber weapons that are known today. The second part points out examples of the most striking recent cyber attacks and uses them as evidences to demonstrate today's importance and dissemination of cyber warfare. Finally, the article sums up pros and cons of the cyber weapons and, in view of these, predicts a significant increase in their use in any future war conflicts.

Keywords: Cyber Warfare, Cyber Security, Middle East, Malware, Stuxnet, Flame, Duqu.

> *"I don't know what kind of weapons will be used in the third world war, assuming there will be a third world war. But I can tell you what the fourth world war will be fought with -- stone clubs."*
>
> Albert Einstein

1 Introduction

"*The United States is fighting a cyber-war today, and we are losing,*" Schneier (2010) proclaimed a former director of National Security Agency (NSA) Mike McConnell in 2010. As a reaction, some American newspapers (Schneier, 2010) have published articles arguing that the threat of a cyber-war is just a hype. However, after a sequence of cyber events of last years, nobody can doubt that the world has entered a new phase of warfare.

Actually, one of the first cyber attacks that was confirmed not to be lead by lonely hackers but on a state level in a large scale was recognised in April 2007 when Russia attacked web pages of Estonian official institutions. Since then, every now and then daily newspapers inform about some new more or less important cyber attacks. For instance, in 2007 China, where blocking of certain websites is a daily routine, three main search engines (Biggs, 2007) were completely blocked in July 2009. Shortly after that incident, websites of official South-Korean and American institutions, banks and media were hit in three waves by a massive DDoS attack. In 2010, first malware aiming at nuclear facilities, Stuxnet, was recognized in Iran and since then, several of its successors have been noticed in the Middle East.

More recently, the frequency and gravity of attacks has been significantly rising. In August 2012, Saudi Arabia national oil company suffered a targeted cyber-attack on their facilities. In October 2012, websites of six US banks including the major ones like JP Morgan and Bank of America underwent a large-scale DDoS attack. (Engleman, 2012) In January 2013, malicious software from a USB flash drive put a US power plant out of order for three weeks. (Fingle, 2013)

Finally, at the beginning of February 2013, just several days before President Obama warned against the US enemies that are trying to *"sabotage our power grid, our financial institutions, and our air traffic control systems"* (The New York Times, 2013) over thirty Western journalists including those from leading US newspapers like The New York Times or The Wall Street Journal have suffered a cyber-espionage according to them from China, (Muskal, 2013) which Chinese officials denied.

Today, almost four years after Mike McConnell's proclamation, a threat of a cyber-war does not seem as such hype anymore. Therefore, if there is another worldwide conflict in the era of the current Western civilization, it will be argued that a great part of such conflict will take place in cyberspace and will be lead by cyber weapons.

Firstly, there will be presented a new type of weapons used in a state-level armed conflict, i.e. cyber weapons. Then, first evidences of such a hypothesis, the members of Stuxnet malware family that have been recognised and already used for a cyber-attack on a national level will be presented. Finally, the perspective role and effectiveness of using different types of cyber weapons and their known representatives against today's threats will be discussed.

Concerning literature review and research methods, the article is of introductory character and as such aspires mostly to present the issue of cyber warfare and to underline its importance today. Therefore, the research methodology is rather descriptive in its first part and argumentative in its second part first in order to introduce the issue, and then to provide evidences for proclaimed thesis, which is a strikingly uprising relevance of cyber warfare. Regarding the high, up-to-date nature of the topic, the chosen literature is constituted mostly by electronic articles retrieved from highly reputed e-databases or by various reports published by recognised computer experts. However, some cornerstone books of cyber warfare theories were used, too.

2 Notion of Cyber War and Its Particularities

2.1 Definition of Cyber Warfare

Now, at the very beginning of this article, key terms need to be specified, since their initial meaning used in the past does not have to correspond to its use today or in the future. First, even though cyberspace has been recognised by U.S. Deputy Secretary of Defence as a new domain of warfare, (Lynn, 2010, pp 97-108) a clear definition of cyber warfare is still missing. Nonetheless, Richard A. Clarke, a former "counter-terrorist tsar" and an expert on a cyber-security, provided a commonly accepted description of a "cyberwarfare": "*actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.*" (Clarke, 2010, p. 292) Although it has been argued that a notion of cyber warfare does not have too much in common with a real war, (Schneier, 2010) one must bear in mind that the term of cyber war still fits into Carl von Clausewitz' definition of war: *"War is thus an act of force to compel our enemy to do our will."* (Clausewitz et al., 1984) Therefore, there is no doubt that a cyberspace is not an equal warfare space to the air, land, sea and space where a real war can be lead.

Nevertheless, the war strategy used in the cyberspace is incomparable to regular strategies used in a physical conflict, since cyber attacks do not have to be obvious right away and even if they are, their authors can be only hardly identifiable. Therefore, it will be really difficult if not impossible to agree upon rules of a war in a cyberspace, much less upon its regulatory compliance unlike most countries have agreed on rules of *jus in bello*. Consequently, the cyber warfare, missing any legal framework, will follow completely different patterns than the typical patterns of a regular armed conflict.

2.2 Categorization of Cyber Weapons

Likewise, cyber weapons are considerably distinct from the weapons used in other warfare spaces. Actually, cyber attacks can be divided into two categories – syntactic attacks that act directly, in other words malicious software, and semantic attacks that aim to modify data (for example on official websites) so that they are wrong but appear to be right at least to a casual viewer. Thus, semantic attacks focus on a user, whereas syntactic attacks direct onto IT facilities. Even though the damages caused by semantic attacks can be of considerable extent, the group of syntactic attacks will be examined in more detail, since syntactic attacks are used more often and cause more damages.

In fact, there are four categories of syntactic attacks (Janczewski, 2008, p. 27): viruses, worms, Trojans and a (distributed) denial-of-service attack (known as a DoS or a DDoS attack). Actually, the last one can be classified also as a semantic attack, since its result is a not working website. The different types of malware differ one from each other according to the target, the way of attack and the aim of attack, they can be coincident in some of these criteria, though. Similarly, the types of particular malware are endowed differently with three crucial factors of cyber attacks – fear factor (reactions caused by an attack), spectacular factor (incurred actual damages) and vulnerability factor (the "easiness" to hack a website of a facility due to the lack of IT security).

Therefore, viruses, a self-injecting and self-reproducing malware that target IT systems and modify or eliminate already existing files in order to paralyze them, cause data loss and freeze or eliminate data knots. Since these malwares can change their digital footprint as well as attach themselves to every file seeming suitable for them, their spectacular and vulnerability factors are very high.

Unlike viruses, worms do not need another file in order to spread, so they can affect a large number of computers in a very short time (a role-model case speaks about 259 000 computers affected in 14 hours (Janczewski, 2008, p. 27). Worms are actually a self-replicating malware that aims the IT systems in order to decrease functionality and the use of data knots in order to paralyze them. Moreover, it can be used for IT espionage; therefore it has an extremely high fear factor as well as vulnerability factor.

Nonetheless, it is usually a Trojan that is used for espionage, since it is a non-injecting malware that enables unauthorized access to hack IT systems in order to track down the activities of hacked systems or in order to alienate data from them. A Trojan can be contained in a trial version of software or in a software updates and be just monitoring user's activity and gathering data, so users do not have to have any clue about having a Trojan in their device for a very long time. Additionally, it can be a part of some complex viruses and worms, so its fear factor as well as its vulnerability factor is very high, while the spectacular factor varies according to a concrete type of Trojan.

Finally, (distributed) denial-of-service attacks (DoS or DDoS) try to break through the communication by short control and information messages that are focused on IT management in order to eliminate partly or wholly the availability of websites, ergo the online services proposed by them, and thus produce chaos and numerous losses. DoS attacks are usually carried out by overloading targeted sites and by generating error-diagnosed messages. However, the demands for websites are not sent directly, the DoS authors make domain name system (DNS) servers, operating only readable web addresses, which give out a number of addresses readable only by a machine. Moreover, the DoS attack can be lead also through unprotected modems or routers of common users which can get disconnected from their internet connection in the end. Thus, the vulnerability factor as well as the fear factor of DoS attacks is enormously high, while their spectacular factor depends on the type of website that has been attacked (considerably high at a bank or PayPal websites). DoS attacks can be spread also by spam emails in order to overwhelm certain e-mail addresses or directly providers of e-mail boxes.

2.3 Methods of Cyber Attacks

Concerning the means most malwares target IT systems, the most popular today is definitely a zero-day attack. Hackers use a zero-day attack once they reveal a so-far unknown vulnerability of a used software or operational system that is not revealed yet to software authors or when there is not yet any available way of defence. Therefore, software users are in danger till software providers issue an upgraded version of software, which will resolve the zero-day issue. Paradoxically, according to the name of the attack, the revelation and correction of a zero-day vulnerability can take hours but also days or years.

Furthermore, hackers sometimes just make a list of vulnerabilities of different software sometimes available online, thus everybody else can use it in order to create a malware targeting a concrete vulnerability at chosen software.

In addition, software producers themselves could integrate the zero-vulnerability while programming the system or they could reveal a concrete description of zero-day vulnerability to different groups of interest or to state entities, while the made-to-measure software has been used elsewhere in a sensitive field like an energy sector.

3 Evidences for a new worldwide conflict: The Stuxnet family

3.1 Appearance of Stuxnet

The best example of malware using the zero-day vulnerability and at the same time, the best example of a malware used as a weapon by a country and not by individuals, is a worm called Stuxnet and its successors. In fact, Stuxnet itself was a pioneer among national cyber weapons, it was also the first part of a complex group of several malwares that complete one each other in terms of their functions as well as in terms of timing of their use having the same objective, though.

Stuxnet malware appeared in IT security rumours for the first time in June 2009 but it was not found outside before June 2010 when it was discovered in Iranian nuclear facilities. However, the very first traces of Stuxnet in Iran nuclear facilities are dated even till 2005. Interestingly, the day before the report on Stuxnet was published by the Kaspersky Lab, the laboratory suffered a DoS attack and a part of its report was destroyed (Fidler, 2011, pp. 56-59)

Finally, Stuxnet turned to be one of the most successful malwares, since it destroyed probably the whole nuclear programme operated on Siemens hardware, although Siemens company denied that any damages had been caused to the users of their equipment. (Langner, pp. 49-51). It spreads mostly via USB flash drives and local networks to the Microsoft Windows operational systems targeting only Siemens controllers, which points out the idea of a potential cooperation between private software or hardware producers and states, since it is believed that Stuxnet is a product of the United States and Israel intelligence agencies. (Falliere, 2011). Actually, Stuxnet was probably the first worm ever that worked without a necessity of any remote control or internet access thanks to a programmable logic controller rootkit (PLC). Even though, its date of death (the day when a worm stops spreading) was supposed to be June 24, 2012, its last attack was noticed in power plants in Iran on December 25, 2012. (Collins, 2012).

Nevertheless, Stuxnet did not spread through massive sources but it attacked with a very narrow focus. Hence, in order to know where to hit, Stuxnet authors probably needed another malware that would collect the information.

3.2 Stuxnet's Little Brothers: DUQU and Gauss

In September 2011, The CrySyS (Laboratory of Cryptography and System Security) of the Budapest University of Technology and Economics discovered an unknown Trojan spyware operating especially in industrial control systems in the Middle East and called it DUQU. The Symantec agency studied the report more profoundly and found out that this zero-day vulnerability spyware (not a worm, since it did not auto-replicate) apparently came from creators of Stuxnet. DUQU's main task was to steal digital certificates, public and private cryptography and to monitor and select data. Later, DUQU's presence in Iran was acknowledged by Iranian authorities. BBC News. (2012a)

Moreover, in August 2012, the Kaspersky Lab detected a Trojan spread mainly in the Middle East area, which tracked down the sensitive data about bank accounts and financial transactions. Newly recognized Trojan named Gauss was apparently created by a state entity, since it has not been used for stealing or fraud but only in order to watch transfers on selected bank accounts. *"More than two thirds of the infections have been discovered in Lebanon, the home base of the political and military Hezbollah organization,"* (Schwartz, 2012) proclaimed Jarno Limnell, Stonesoft director of cyber security.

In September 2012, several computer security companies informed about a new cyber espionage malware called Shamoon that acted in a very similar way like Gauss did but in the oil and energy sector. A self-injecting and a self-erasing virus attacked approximately 30,000 workstations of Saudi Aramco, which spent a week by renewing their services. (Symantec, 2012) However, even South Korean banks were hit by Shamoon attack recently, showing the danger of a boomerang effect of cyber weapons.

3.3 The Missing Piece of Puzzle Discovered: Meet Flame

Nonetheless, the biggest piece of puzzle came in May 2012. The Kaspersky Lab brought a report about the existence of the most powerful malware so far, calling it Flame. It is pretty difficult to answer what kind of malware Flame is because it is a kind of everything: *"It is a backdoor, a Trojan, and it has worm-like features, allowing it to replicate in a local network and on removable media if it is commanded so by its master.*" (Zetter, 2012) Similarly to its ancestor, Stuxnet, Flame focuses on the surveillance of infected IT systems using the zero-day vulnerability.

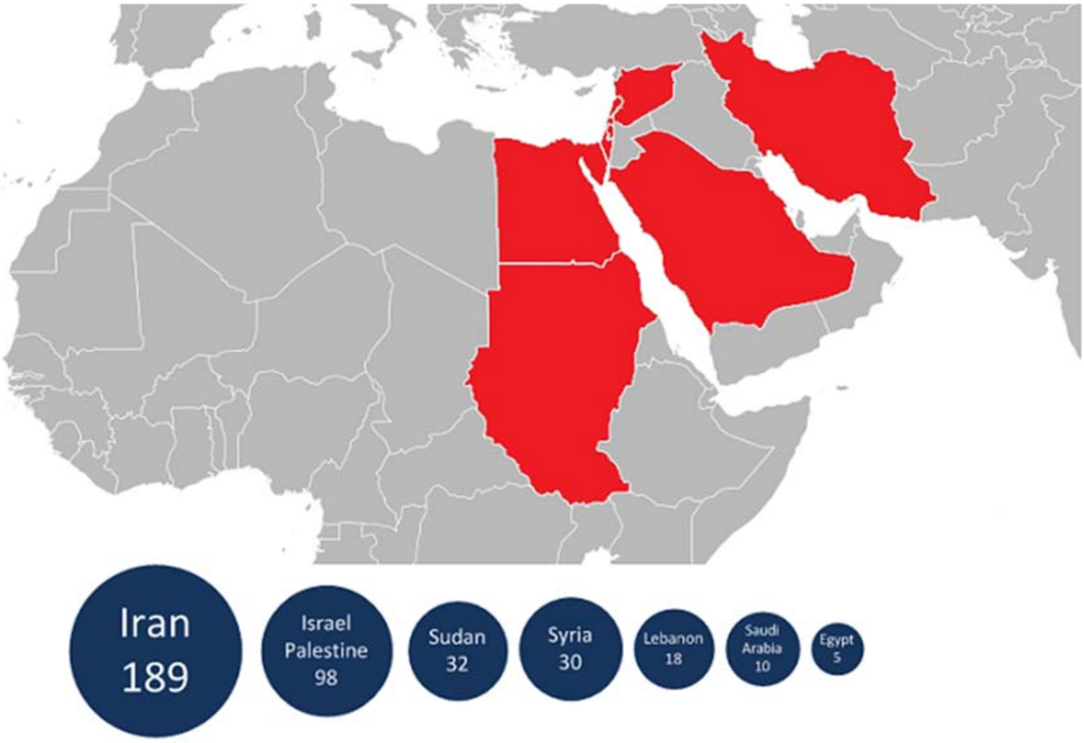

Fig. 1. *Kaspersky Lab report on the number of Flame recorder attacks*. Source: (Kaspersky Lab, 2012).

Indeed, Flame can do almost everything. Besides the customary recording of data and monitoring the process running in a computer, it can also take screenshots of running applications, record of audio data through an internal microphone or get connected through a Bluetooth device of host computer to another devices and monitor their activities, too.

Flame is not only an extremely big malware of 20 megabytes but also an exceptionally complicated programme. It is written partly in a form of C++ language, Lua scripting, whose *"development cost is over 3000 lines of code, which for an average developer should take about a month to create and debug,*"(CRySyS Lab, 2012) says the CrySyS Lab report. What is even more interesting is that Flame, circulating probably from March 2010, the time when Stuxnet was discovered, is believed to be rather a back-up plan: *"Hence, we believe Flame to be a parallel project, created as a fallback in case some other project is discovered."* (CRySyS Lab, 2012) Since Flame and so-called Tided platform i.e. Stuxnet/Duqu work on different platforms, although on the same principle using the same methods, it seems like creators of Stuxnet launched Flame, once Stuxnet was publically revealed.

Yet, Flame as a widely spread tool which appeared even in French presidential office, BBC News. (2012b) probably needed also some smaller, more specialized complement. In July 2012, Kaspersky Lab discovered a Mini Flame, a highly specialized malware recognized only in several dozens of infections (maximum 50 – 60 worldwide). (Securelist, 2012) *"Since it [miniFlame] is known to have worked both as part of Flame and as part of Gauss and since it shares its C&C servers with Flame, we believe that in most cases SPE was installed from C&C servers onto systems that were already infected with Flame or Gauss,"* (Securelist, 2012) thus, miniFlame is considered to be one of the last parts of the cyber puzzle destined to Iran and the Middle East area in general. Finally, the very recent discover of another malware in Iranian IT devices called Wiper can testify that some pieces may still be missing.

4 Conclusion

In the warfare of the 21st century, cyber weapons will be definitely used more and more in terms of frequency as well as amplitude. They are relatively cheap, especially for countries with a developed IT sector, their authors could be hardly proven to be guilty, since direct evidences of hacking one's system are practically unable to be tracked down, and their use is not limited by any international legal framework for now. Therefore, if it is possible to use a hard power without being seriously accused on the base of direct evidences, which is exactly the power cyber weapons have, therefore countries will not hesitate and use it.

Moreover, the rising number and weight of recently revealed cyber attacks represented mostly by the family of Stuxnet and Flame malwares, whose origin is probably common and not private but national pointing out especially the USA - Israel direction, is a strong evidence for sharply evolving cyber warfare, especially in the world where evident hard power, whose author is known, is not convenient to use because of international relations. Besides, the revealed attacks make one think that there is a few of ongoing malware attacks that have not been discovered yet.

Nonetheless, cyber weapons have their limits, too. For instance, they can have a boomerang effect that is highly dangerous like in the example of South Korea when authors of malware or its allies did not have appropriate protection against the pieces of their own work. In addition, the use of internet and digitalization of (nuclear) energy sector is rather limited like in the case of North Korea.

In any case, the danger of cyber attacks from different actors will rise and due to the lack of a clear international mechanism for cyber security, (as vast majority of current international security mechanisms do not cover the area of cyber security), each country shall create and further develop its own protective system, a sort of its own "cyber army". For instance, the United States of America has created already in 2009 a system called Cyber Command, however, the Czech Republic does not lag behind and this May, it has created the National Centre for Cyber Security called CERT in Brno. CERT should monitor all possible risks to cyber security, ensure cooperation between different agencies and institutions dealing with cyber security on national as well as on international level and develop new standards and tools of cyber security system. Thus, a system of national cyber security for the Czech Republic has been already launched; nevertheless, it should get more attention from public as well as from the government especially in terms of finances.

To conclude, today's world has been currently undergoing a new paradigm shift where cyber weapons and cyber warfare are taking over the place of regular weapons and warfare that dominated so far. It is obvious that a real world-wide cyber conflict between two countries with equally high developed IT sector has not burst out yet. However, when it does, it will be probably the last sophisticated conflict before these countries take up their stone clubs again.

References

BBC News. (2012a, June 8). *Flame malware makers send 'suicide' code.* Retrieved from http://www.bbc.com/news/technology-18365844.

BBC News. (2012b, May 31). *Flame: Israel rejects link to malware cyber-attack.* Retrieved from http://www.bbc.com/news/technology-18277555.

Biggs, J. (2007, October 18). *Cyberwar: China Declares War On Western Search Sites.* Retrieved from http://techcrunch.com/2007/10/18/cyberwar-china-declares-war-on-western-search-sites/.

Carr, J. (2011). *Inside Cyber Warfare: Mapping the Cyber Underworld.* Sebastopol, CA: O'Reilly Media.

Clarke, R. A., Knak, R. K. (2010). *Cyber War: The Next Threat to National Security and What to Do about It.* New York: HarperCollins.

Collins, S., McCombie, S. (2012). Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism*, 7(1), 80-91.

CRySyS Lab. (2012, 28 May). sKyWIper: A Complex Malware for Targeted Attacks. Budapest University of Technology and Economics. Retrieved from http://www.crysys.hu/skywiper/skywiper.pdf.

Engleman, E. (2012, December 20). *Major Banks Under Renewed Cyber Attack Targeting Websites.* Retrieved from http://www.bloomberg.com/news/2012-12-20/major-banks-under-renewed-cyber-attack-targeting-websites.html.

Erdbrink, T. (2012, April 23). Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals From Internet. *The New York Times.* Retrieved from http://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html?_r=0.

Esposito, M. K. (2012). Quarterly Update on Conflict and Diplomacy. *Journal of Palestine Studies*, 42(1). Retrieved from http://www.palestine-studies.org/files/pdf/jps/9765.pdf.

Farewell J. P., Rohozinski R. (2011). Stuxnet and the Future of Cyber War. *Survival: Global Politics and Strategy*, 53(1), 23–40.

Fidler, D. P. (2011). Was Stuxnet an Act of War? Decoding a Cyberattack. *IEEE Security & Privacy*, 9(4), 56-59.

Finkle J. (2013, January 16). *UPDATE 1-Malicious virus shuttered U.S. power plant -DHS. Reuters.* Retrieved from http://www.reuters.com/article/2013/01/16/cybersecurity-powerplants-idUSL1E9CGFPY20130116.

Howard, M., Paret, P. (1984). *On War.* New Jersey: Princeton University Press.

Janczewski, L., Colarik, A. M. (2008). *Cyber Warfare and Cyber Terrorism.* Hershey: Information Science Reference.

John, A. J., Ronfeldt, D. (1993). Cyberwar is Coming! *Comparative Strategy*, 12(2), 141–165.

Kaminski, R. (2012). Clash of Interpretations: Cyberattacks as “Weapons of Mass Destruction” In *The 2012 Annual Meeting of the American Political Science Association.* Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2107008.

Kaspersky Lab. (2012, June 11). Resource 207: Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected. Retrieved from http://www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected.

Kindlund, D. (2012, May 30). Flamer/sKyWIper Malware: Analysis. *FireEye*. Retrieved from http://www.fireeye.com/blog/technical/targeted-attack/2012/05/flamerskywiper-analysis.html.

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy*, 9(3), 49-51.

Lee, D. (2012, May 29). Flame: Massive Cyber-Attack Discovered, Researchers Say. *BBC News*. Retrieved from http://www.bbc.com/news/technology-18238326.

Lynn, W. J. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*. 97–108.

Matrosov, A., Rodionov, E., Harley, D., Malcho, J. (2010). *Stuxnet Under the Microscope*. Retrieved from http://www.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

Muskal, M., Guynn, J. (2013, February 1). Hackers target Western news organizations in China. *Los Angeles Times*. Retrieved from http://articles.latimes.com/2013/feb/01/business/la-fi-china-hacking-20130201.

Nakashima, E. (2012, June 20). Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. *The Washington Post*. Retrieved from http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.

Nicolas F., Liam O. M., Eric, Ch. (2011) *W32. Stuxnet Dossier. Symantec Report.* Retrieved from http://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf.

SciencePages. (2013, March). *Cyber Security*. Retrieved from http://sciencepages.ca/wp-content/uploads/cybersecurity.pdf.

Schneier B. (2010, July 10). *Threat of 'cyberwar' has been hugely hyped*. Retrieved from http://edition.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/index.html.

Schwartz, M. J. (2012, August 9). *Flame 2.0: Gauss Malware Targets Banking Credentials*. Retrieved from http://www.darkreading.com/attacks-and-breaches/flame-20-gauss-malware-targets-banking-credentials/d/d-id/1105727?.

Securelist.com. (2012, October 15). *MiniFlame aka SPE: "Elvis and his friends"*. Retrieved from http://www.bbc.com/news/world-europe-20429704.

Silverstein, R. (2012, May 29). *Flame: Israel's New Contribution to Middle East Cyberwar*. Retrieved from http://www.richardsilverstein.com/2012/05/28/flame-israels-new-contribution-to-middle-east-cyberwar/.

Symantec. (2012, August). The Shamoon Attacks. Retrieved from http://www.symantec.com/connect/blogs/shamoon-attacks.

Symantec Official Blog (2012, May 30). *Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East. (Web log post).* Retrieved from http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east.

The New York Times. (2013, 12 February). *President Obama' State of Union speech*. Retrieved from http://www.nytimes.com/2013/02/13/us/politics/obamas-2013-state-of-the-union-address.html?pagewanted=all.

Zetter, K. (2012, May 29). Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers. *Wired*. Retrieved from http://mashable.com/2012/06/04/flame-malware/.