Science Journal of Business and Management
2015; 3(1-1): 39-45
Published online December 30, 2014 (http://www.sciencepublishinggroup.com/j/sjbm)
doi: 10.11648/j.sjbm.s.2015030101.17
ISSN: 2331-0626 (Print); ISSN: 2331-0634 (Online)

Age of cyber crime and culture of security

András Keszthelyi

Keleti Faculty of Business and Management, Óbuda University, Budapest, Hungary

Email address:
Keszthelyi.Andras@kgk.uni-obuda.hu

To cite this article:
András Keszthelyi. Age of Cyber Crime and Culture of Security. *Science Journal of Business and Management.* Special Issue: The Role of Knowledge and Management's Tasks in the Companies. Vol. 3, No. 1-1, 2015, pp. 39-45. doi: 10.11648/j.sjbm.s.2015030101.17

Abstract: Entering into the "Information Age" brought us some new challenges. One of them is cyber crime and cyber warfare shooting upwards: instead of formal law which became a dead letter, nowadays club law dominates on the Network. How can enterprises and people manage their own security? I have been collecting several news of security incidents for fifteen years. Analysing this systematic collection some characteristic attributes of the new era can be identified: traditional definitions and concepts related to security do not work anymore. Both of technology and formal knowledge are necessary but not enough to survive. Organisations as well as individuals must (or have to) develop their own culture of security.

Keywords: Cyber Crime, Cyber Warfare, IT Security, Culture of Security

1. Introduction

I have been collecting news related to security incidents of any kind for more than one and a half decade. This collection originates from a wide range of sources from professional journals and papers to general news sites. The collection is, of course, far from being complete, not to speak about incidents that were and are not communicated to the public.

The main goal of this collection is to show the trends. Looking at the collection one cannot think of these incidents as separated random accidents. It shows that we are in an alarming situation, a new era has started.

This new era is the age of cyber crime and, what is more, cyber warfare, even if some experts try to deny that: GData (2012) said about the security trends of 2013 that „cyber war not on the horizon". They would have been right if they had meant that cyber war was not on the far horizon, but was taking place here.

Looking at the series of security related incidents, quite a big set, some general conclusions can be made. First of all: the paradigm is under change. This means that some new questions must be asked about security.

In this paper I include only some important or relevant or interesting examples from the past fifteen years that represent the wide range of different categories. Cyber crime and warfare has become part of our everyday life.

Can we, private persons and employees and enterpreneurs, cope with this challenge or not? If yes, what is the winning strategy (if such a strategy exists at all)?

2. The New Era

2.1. Paradigm Shift

The present age is often called as information age, because not only the amount of data stored digitally in computerized environments increases but our dependency of these data shoots upwards as well. We use computers and the network in almost all fields of life, both in official and in private life, computers and The Network became part of life.

The revolutionary new technology and its becoming general results in a surprising situation: old axioms, rules and regulations do not work any more.

For example, people can make as many copies of a digitally stored book, song, movie as they want, in an infinitesimally short period of time, and these copies are not only of the equal quality as the original ones but they can be transferred to any distance and to any other people, too, and there is no physical abrasion.

A new phenomenon has appeared: cyber crime and warfare. This phenomenon is well characterized even by the increasing number of Google results for "cyber crime". Google listed 250 results for the year 2013 while for the first ten months of 2014 it listed 274 titles (cca. 330 for the whole year, 32% increase).

Taking a look at the number of the results for "cyber war" the situation is very similar.

"The Pentagon sees the internet in terms of a military adversary (…) This explains the confrontational language in the document which speaks of 'fighting the net'; implying that

the internet is the equivalent of 'an enemy weapons system.'" Whitney (2006) writes citing the BBC, eight years ago.

This is not a phrase. According to latest news the head of the NSA, Admiral Michael Rogers, says: "China and a number of other countries has infiltrated the computers of critical industries in the United States to steal information that could be used in the planning of an attack, according to the director of the National Security Agency." (Nakashima, 2014.)

In 2007 Mark Hall, the director of the international information assurance program for the Defense Department of the United States said: "In the event of a massive cyberattack against the country that was perceived as originating from a foreign source, the United States would consider launching a counterattack or bombing the source of the cyberattack", Messmer cites Hall (2007).

According to the formal law in the United States the president must receive the approval of the Congress to order starting a military action. So the interesting question is: are cyber attacks military actions or not? Experts try to clear these theorietical and legal problems in the Tallinn Manual (Schmitt, 2013).

2.2. Differences between Traditional and Virtual World

First of all let's see how things work in the traditional world.

First: Let us suppose you have a car. If your car were stolen you would recognize it easily observing the simple fact that the car would not be at the place where you left it. The converse of the theorem is also true. While your car stands at the very place where you have left it you may know that it has not been stolen (yet).

Second: If your car has been stolen you will know that the thief was physically and personally on the spot, at the very time when it has been stolen.

Third: In case of any kind of physical aggression you can realize where the beat, cut, arrow, bullet or intercontinental ballistic missile has come from. Or at least the ballistic expert will be able to determine it.

Fourth: Bullets and missiles of modern firearms can be used only once, obviously. When they have reached their target they will explode and so they will annihilate not only the target but themselves, too.

Fifth: You may have secure places to hide your secrets (or any other staff) and keep them safe until you are totally defeated.

In the virtual world things work differently.

First: Having all of your data in your computer or in your network does not mean that your data is not stolen. On the contrary: your data may well be stolen, perhaps more than one. Almost all data thefts may be examples here, especially two: in 2005 an undetermined amount of data, but at least 20 GB was stolen from Kennedy Space Center. (Epstein, 2008.) In 2012 the design documentation of the the F35 Joint Strike Fighter was stolen from the network of BAE Systems. (Leppard, 2012).

Second: If someone could manage to steal your sensitive and valuable data or could manage nearly any kind of intrusion that does not mean that the attacker must have necessarily been anywhere at any time.

Third: In the virtual world there are no 'ballistic experts', usually you cannot decide where the attack originated from. Even if you have an IP address as the origin of the attack you may not (and must not) be sure that it is the real IP address of the real attacker. This is why news about data thefts are usually contains conditionals "probably Chinese hackers", "data travelled to Taiwan or somewhere else through Taiwan computers" etc., for example.

Fourth: You have real chances to catch a malware started against your system. Then you can disassembly the software to analyse it and to further develop it to send it back to the sender, or your other enemies. This happened with the Stuxnet virus. Somehow it infected a lot of companies in the world and even in the US, Chevron for example. (King, 2012.) The Duqu malware, too, is based on the Stuxnet virus. (Bencsáth, 2011.)

Fifth: In the virtual world there is "No place to hide". (Greenwald, 2014.) Even if your computer has no network interfaces and is kept under continuous physical control, even in those circumstances the NSA, for example, may be able to eavesdrop on you, according to latest news by (Sanger and Shanker, 2014).

There are additional specialities because of the nature of the PC architecture: you cannot be sure that your computer is only yours without any backdoors. Then your (virtual) clients may not be those you think they are.

Obviously, in such circumstances it is hard to realize even the fact that your computer system has been compromised and/or your data has been stolen. If you have successfully realized that there was an attack against your system it will not be an easy job do know who the attacker was. And it is significantly harder to prove that in a good-for-a-prosecution way, because the byte-level content of a hard drive will not prove (or confute) anything, in alone at least.

After so many differences we can find at least one similarity: both in the traditional world and in the virtual one always the winner decides who is the hero and who is the criminal.

3. Security Incidents

My collection is far from being complete. Even in this case the material is enough to find typical attributes and organize the incidents into different subsets based on their general similarities from the functional point of view. There may be other classifications, too, and some incidents might be listed in different groups. Only a few examples are listed to illustrate the very different kind of countinuous threats.

3.1. Cyber Warfare

The Estonian government was considering the relocation of a Soviet World War II memorial (…) from its original place to the Tallinn Military Cemetery. (…) The distributed denial of service (DDoS) attacks on Estonia in 2007 have gone down in history as one of the largest coordinated cyberattacks." (Joywang, 2012).

It caused significantly more harms to Estonia than if Russia

had introduced financial and/or business sanctions against the country. (Schmidt, 2013) Because of the above discussed attributes of the virtual world of computer networks experts could prove in only one case the Russian origin of the attack.

"Stuxnet, the computer worm which disrupted Iranian nuclear enrichment in 2010, is the first instance of a computer network attack known to cause physical damage across international boundaries." (Lindsay, 2013.)

"The Stuxnet virus, which has attacked Iran's nuclear facilities and which Israel is suspected of creating, has set back the Islamic Republic's nuclear program by two years, a top German computer consultant who was one of the first experts to analyze the program's code told The Jerusalem Post on Tuesday." Katz (2010). Later investigations showed that the virus got into the closed network on a usb memory stick.

Robert Elder Jr., a three-star general was appointed as the first cyber-general in the US. The Cyber Command of would have over twenty thousand experts and engineers. (Carrol, 2008).

F-Secure says that the participation and the role of governments in cyber attacks becomes stronger and stronger. (F-Secure, 2012).

"The U.S. military is increasing its budget for cyber-warfare and expanding its offensive capabilities, including the ability to blind an enemy's radar or shut down its command systems in the event of war, according to two defense officials." (Michaels, 2013).

3.2. Industrial and/or Military Espionage

An attacker penetrated the network at the Marshall Space Flight Center in 2002 and managed to steal secret data on rocket engine designs. It was believed that these data was directed to China. (Epstein, 2008).

A malicious software, stame.exe by name, was installed in the Kennedy Space Center by cyber-criminals in 2005. The malware sent an undetermined, but at least compressed 20 GB, amount of data to Taiwan (or somewhere else through Taiwan). (Epstein, 2008).

"German domestic security agencies believe that Chinese hackers (...) installed Trojan spy programs (...) on several computers at the Federal Chancellery, the Foreign Office, the Ministry of Economics and Technology, as well as the Federal Ministry for Education and Research.", the cover story of Der Spiegel, titled "The Yellow Spies: How China Spies Out German Technology" is cited by Gartzke in The Weekly Standard. (Gartzke, 2007)

Perhaps Chinese hackers got into the network of BAE Systems and could steal the design documentation of the F35 Joint Strike Fighter aeroplane. "Experts fear the jet's radar capabilities could have been compromised." (Leppard, 2012).

3.3. Everyday Life

According to researchers modern, computer controlled cars may be hacked, too. "Over a range of experiments, both in the lab and in road tests, we demonstrate the ability to adversarially control a wide range of automotive functions and completely ignore driver input – including disabling the brakes, selectively braking individual wheels on demand, stopping the engine, and so on." (Koscher, 2010). Another research in this field is (Checkoway 2011). There is no proof about that the death of Lady Diana and Jörg Haider would have been in any kind of connection of these possibilities of car hacking.

Not only cars may be hacked but airliners, too. On the Hack in the Box (#HITB2013AMS) security conference in Amsterdam Hugo Teso demonstrated, citing his abstract "how to remotely attack and take full control of an aircraft (…) The complete attack will be accomplished remotely, without needing physical access to the target aircraft at any time." (Storm, 2012)

"Barnaby Jack showed how an attacker with a laptop, located up to 50 feet from a victim, could remotely hack a pacemaker and deliver an 830-volt shock." (Storm, 2012). Last year former vice president Dick Cheney asked his doctors to switch off the remote wireless access to his pacemaker to avoid a possible outrage that could have killed him.

3.4. Critical Infrastructure

There was an incident that led to the failure of a pump at a water system in Springfield, Illinois, United States. It was considered the first known attack against public infrastructure. Later investigations could find no proofs of being so. (Krebs, 2011).

After three years, in 2014 the United States declared that it was (and is?) possible. "China and 'one or two' other countries are capable of mounting cyberattacks that would shut down the electric grid and other critical systems in parts of the United States, according to Adm. Michael Rogers, director of the National Security Agency and head of U.S. Cyber Command." (Dilanian, 2014.)

3.5. Political Espionage

In January, 2010, in Dubai a Hamas leader was assassinated by an Israeli hit sqad. Previously the laptop of al-Mabhouh had been infected with a Trojan program that had made it possible for the attackers to get access to the victim's emails. (Leyden, 2010).

In December Google detected a highly sophisticated cyber attack aiming Google's corporate infrastructure. The attackers wanted to get access to the mailboxes of Chinese human rights activists. Investigations diagnosed that the attack was not successful. (Google, 2010).

3.6. User Data

2009, Hotmail. The list of stolen passwords initially contained 10,028 entries. After cleaning up the list 9843 valid passwords remained, of which 8931 (90%) are unique. The most common password was: 123456. (Calin, 2009.)

2009, Rockyou. In December 2009 32 million passwords were revealed by a successful SQL injection attack. Passwords were stored in plaintext form in the database which is a serious carelessness. "The data provides a unique glimpse into the

way that users select passwords and an opportunity to evaluate the true strength of these as a security mechanism. In the past, password studies have focused mostly on surveys. Never before has there been such a high volume of real-world passwords to examine." (ADC, 2010.)

2011 was the year of great data breaches. In March 40 million RSA-users' accounts, in April 20 million Google-accounts, in May 100 million Sony accounts were compromised, according to Websense (Websense, 2011) report.

In the summer of 2012 a list of 450,000 usernames and plaintext passwords were revealed from Yahoo. According to (Nilsson, 2012) the top 10 passwords were: 123456, password, welcome, ninja, abc123, 123456789, 12345678, sunshine, princess, qwerty. The top 10 base words were: password, welcome, qwerty, monkey, jesus, love, money, freedom, ninja, writer.

In the same year, 2012, the data of 6,5 million users were stolen from LinkedIn.

In 2013 Adobe was the victim and about 38 million user records were stolen. (Ducklin, 2013.)

The main problem is that having so many real life user passwords you can analyse the password selecting habits of users, the typical password structures to develop more efficient and sophisticated password cracking methods. In addition, user carefulness is in vain if their passwords are stored in plain text.

3.7. Anti-Virus Software is not Enough

The Gh0st RAT (remote access tool) incident. Researchers believe the tool was developed in China. It allows the attackers to steal date from the victims' computers in a sophisticated mode. Researchers found that an extensive cyber espionage campaign was in progress, using Gh0st RAT, targeting more than one thousand computers in 103 countries, all of them was at important points of media, political, enterprise offices. This malware was found even in 2002, too. (Kirk, 2013).

Sony BMG Music Entertainment was distributing music CDs with a software that installed a rootkit onto computers without the consent or even the knowledge of the user. Once the rootkit software was loaded a hacker could gain (and maintain) access to the computer of the victim also without any knowledge of the owner of the computer. "What do you think of your antivirus company – Schneier asks –, the one that didn't notice Sony's rootkit as it infected half a million computers? And this isn't one of those lightning-fast internet worms; this one has been spreading since mid-2004 [i.e. for one and a half year]." (Schneier, 2005.)

3.8. Random Accident

"In 2008, the then-unemployed man was using Skype (...) when he dialed a random number and then entered the code "123456" (…) Although he didn't realize what he had done, the man was granted access to the French central bank's debt service." (Weitzenkorn, 2012)

3.9. Common Crime

A Frenchman succeeded in breaking into even Barack Obama's twitter account in 2010. The man "managed to break into the accounts by searching information that is most commonly used for passwords, such as birth dates or pet names, on social networking sites. He lives with his parents and has no college degree, and has not had any special computer training." (Mesquita, 2010.)

The case of iCloud nude celebrities from the near past also might be mentioned.

3.10. Financial Organizations

Unknown attackers succeeded in getting into the computers of the International Monetary Fund. They had been able to search for and download data for months before the attack itself was noticed. The IMF "possesses sensitive data on a lot of countries that (...) are, in the words of one fund official, 'political dynamite in many countries.' It was unclear what information the attackers were able to access." (Sanger, 2011).

A very strange phenomenon occurred in the U.S. stock market in 2012. "A single mysterious computer program that placed orders – and then subsequently cancelled them – made up 4 percent of all quote traffic in the U.S. stock market last week, according to the top tracker of high-frequency trading activity. The motive of the algorithm is still unclear." (Melloy, 2012). We can only imagine what could happen if such a program would be set free.

3.11. Highly Sophisticated Software Tools

The Gh0st RAT malware was mentioned above.

Duqu malware was found by the researchers of the Crysys Lab at the Budapest University of Technology and Economics. The malware was developed on the basis of the Stuxnet virus and optimized for industrial espionage. (Bencsáth, 2011). Duqu uses a new digitally signed windows driver signed by a hardware manufacturer in Taiwan.

The MiniDuke, SkyWiper (Flame) and Uroboros malwares ought to be mentioned here.

3.12. Social Media, Human Factor

First of all Facebook, but social media, too, in general, has become the hunting field of data phising. Cyber spies managed to set up a fake Facebook-account for admiral James Stavridis (NATO's 16th Supreme Allied Commander Europe) hoping that his real life friends and juniors at NATO would answer the friend requests that would lead to getting access to the personal data of their FB profiles. (Hopkins, 2012).

A lot of well known examples of different kinds of data phishing, Nigerian cheats, ransomwares, etc. ought to be mentioned in this section.

4. Countermeasuers

Websense warned us: "It's no longer a question of 'if' but 'when'! Not all companies will get breached, but may will."

(Websense, 2011)

First of all, as our situation is something like we lived in the Wild West, do not wait for the police to defend you. It is of no use if an investigation concludes that you were right and some private, mafia or state criminals defeated your enterprise but in the meantime you went bankrupt. So you must defend yourself, both as a private person and a member of a company.

The obvious part of the possibilities of self-defence is to apply all the countermeasures that you are allowed to and obliged to do. The use of all the possible technological, organizational and regulational tools, industry best practices are not an option, that is a must.

Risk analyses has been an important tool to reduce the costs while keeping the level of security. As our systems becomes more and more complicated the number of input factors and rules, not to speak about the number of interactions between them, increases as well. Handling these interactions may be problematic, because it is difficult to see through the combined effect of the large amount of factors even for experts. (Tóth-Laufer et al, 2013.)

Because an increasing part of attacks takes aim at the human factor, it must be strengthened, naturally. This means learning and teaching, first of all.

Teaching, training and further training in the fields of IT security and – it is more important – information security is a necessary pre-requisite of making the enterprise more secure. There are three reasons why education in this field is so important.

Firstly, regulations are worth as much as employees keep them. The more they understand the more they will keep of them.

Secondly, the field of IT goes ahead very fast. What one knows today that will not be enough tomorrow.

Thirdly, even basic knowledge of IT seems to be imperfect. The level of the IT knowledge of the present-day students, at least here in Central Europe, is far from being ideal, as two surveys of Kiss prove that. (Kiss, 2011, 2012a, 2012b)

What else, or what more could be done? The knowledge your employees (or you) actually have may easily be not enough and/or obsolete. Training is a good investment, but seems not to be sufficient. A better strategy is to develop the culture of security at the enterprise. Individual factors influence individual behaviour in relation to organisational safety and security. Good culture means less opportunity for risk behaviour. (Lazányi, 2014)

5. Conclusions

As not only the amount of data stored in digital form in computers and in computer networks increases day by day but our dependency of it, too, IT becomes more and more important part of our everyday life. This results in a paradigm shift, and an interesting and dangerous consequence is that crime and warfare has appeared on the virtual horizon of The Network.

Taking a look at the long row of the known security incidents the most important differences between the traditional, old world and the new networked, virtual world may be discovered. The old rules, we were accustomed to, are not valid anymore.

The new era means new challenges. We, both as private persons and members of companies, must face with dangerous situations, and we must fight for our security.

To win this fight technology itself is not enough. To do well in such a quickly changing field we must learn and teach our employees, but that may not be sufficient. We ought to develop the culture of security as a response to the new challenges.

“Believe in God, and keep the gunpowder dry!”

References

[1] Bencsáth, B. et al. (2011), Duqu: A Stuxnet-like malware found in the wild. http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf, Oct. 2011.

[2] Calin, B. (2009), Statistics from 10,000 leaked Hotmail passwords, Acunetix Web Application Security, http://www.acunetix.com/blog/news/statistics-from-10000-leaked-hotmail-passwords/

[3] Carrol W. (2008), The New Cyber General, http://defensetech.org/2008/01/02/the-new-cyber-general/

[4] Checkoway et al. (2011), Comprehensive Experimental Analyse of Automative Attack Surfaces, USENIX Security, http://www.autosec.org/pubs/cars-usenixsec2011.pdf

[5] Consumer Password Worst Practices by The Imperva Application Defense Center (ADC), (2010), http://www.imperva.com/docs/wp_consumer_ pass word_worst_practices.pdf

[6] Dilanian, K. (2014), NSA Director: Yes, China Can Shut Down Our Power Grids. Business Insider, 20.11.2014. http://www.businessinsider.com/nsa-director-yes-china-can-shut-down-our-power-grids-2014-11

[7] Ducklin, P. (2013), Anatomy of a password disaster - Adobe's giant-sized cryptographic blunder, Naked Security - Award-winning computer security, news, opinion, advice and research from SOPHOS, 4.11.2013. https://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/

[8] Epstein K. (2008), Network Security Breaches Plague NASA, in: Bloomberg Businessweek Magazine, 19. Nov. 2008. http://www.businessweek.com/stories/2008-11-19/network-security-breaches-plague-nasa, downloaded from Google cache, Feb. 2014.

[9] F-Secure (2012), Threat Report H1 2012, https://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2012.pdf

[10] Gartzke U. (2007), Outrage in Berlin Over Chinese Cyber Attacks, in: The Weekly Standard, 31/8/2007. http://www.weeklystandard.com/weblogs/TWSFP/2007/08/outrage_in_berlin_over_chinese.asp

[11] GData (2012), IT security trends in 2013: cyber war not on the horizon. http://sa.gdatasoftware.com/jp/security-labs/news/news-details/article/3029-it-security-trends-in-2013-cy.html, Dec. 2012

[12] Google (2010), A new approach to China, Google Official Blog, http://googleblog.blogspot.hu/2010/01/new-approach-to-china.html

[13] Greenwald, G. (2014), No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. Henry Holt and Company, New York. ISBN 978-1-62779-073-4.

[14] Hopkins, N. (2012), China suspected of Facebook attack on Nato's supreme allied commander, in: The Guardian Online, http://www.theguardian.com/world/2012/mar/11/china-spies-facebook-attack-nato

[15] Joywang (2012), The 2007 Estonian Cyberattacks: New Frontiers in International Conflict, On Cyber War – Freshman Seminar 43z – Internet Law, http://blogs.law.harvard.edu/cyberwar43z, downloaded 12/22/2012.

[16] Katz, Y (2010), 'Stuxnet virus set back Iran's nuclear program by 2 years'. The Jerusalem Post, 15.12.2010. http://www.jpost.com/Iranian-Threat/News/Stuxnet-virus-set-back-Irans-nuclear-program-by-2-years

[17] King, R. (2012), Virus Aimed at Iran Infected Chevron Network, The Wall Street Journal, 9.11.2012. http://online.wsj.com/articles/SB10001424127887324894104578107223667421796

[18] Kirk J. (2013), Gh0stRAT malware attacks continue, researcher says. In: Computerworld, http://www.computerworld.com/s/article/9238640/Gh0stRAT_malware_attacks_continue_researcher_says?taxonomyId=17

[19] Kiss, G. (2011), A Comparison of Informatics Skills by schooltypes in the 9-10th grades in Hungary, in: International Journal of Advanced Research in Computer Science, Volume 2, No. 2, pp. 279-284.

[20] Kiss, G. (2012a), Measuring Computer Science Knowledge Level of Hungarian Students specialized in Informatics with Romanian Students attending a Science Course or a Mathematics-Informatics Course, in: TOJET: The Turkish Online Journal of Education Technology, Volume 11, Issue 4, pp. 222-235. Oct. 2012.

[21] Kiss, G. (2012b), Measuring Hungarian and Slovakian Students' IT Skills and Programming Knowledge, in: Acta Polytechnica Hungarica, Volume 9., No. 6, 2012, ISSN: 1785-8860, pp. 195-210.

[22] Koscher et al. (2010), Experimental Security Analysis of a Modern Automobile, in: IEEE Symposium on Security and Privacy, Oakland, CA, http://www.autosec.org/pubs/cars-oakland2010.pdf

[23] Krebs (2011), DHS Blasts Reports of Illinois Water Station Hack. http://krebsonsecurity.com/2011/11/dhs-blasts-reports-of-illinois-water-station-hack/

[24] Lazányi, K. (2014). A biztonsági kultúra [The Culture of Security], VIKEK, Szeged, in print.

[25] Leyden J. (2011), Dubai assassins used email trojan to track Hamas victim – Mossad kill squad tried poison before hotel lock-hack, In: The Register, http://www.theregister.co.uk/2011/01/05/mossad_dubai_assassination/

[26] Lindsay, J. (2013), Stuxnet and the Limits of Cyber Warfare, Security Studies, 22:3, 365-404, DOI: 10.1080/09636412.2013.816122, http://dx.doi.org/10.1080/09636412.2013.816122

[27] Leppard, D., 2012. Chinese steal jet secrets from BAE, in: The Sunday Times, http://www.thesundaytimes.co.uk/sto/news/uk_news/National/article991581.ece

[28] Melloy, J. (2012), Mysterious Algorithm Was 4% of Trading Activity Last Week, CNBC, http://www.cnbc.com/id/49333454

[29] Mesquita, R. (2010), Frenchman convicted for hacking Obama, http://www. boston. com/business/technology/articles/2010/06/25/frenchman_ convic ted_ for_hacking_twitter/, 25 June 2010.

[30] Messmer, E. (2007), U.S. cyber counterattack: Bomb 'em one way or the other, in: NetworkWorld, IDG, http://www.networkworld.com/news/2007/020807-rsa-cyber-attacks.html?page=2

[31] Michaels, J. (2013), Pentagon expands cyber-attack capabilities, in: USA Today http://www.usatoday.com/story/news/nation/2013/04/21/pentagon-expanding-offensive-cyber-capabilities/2085135/

[32] Nakashima, E. (2014), NSA warns China could take out US power grid. http://www.afr.com/p/world/nsa_warns_china_could_take_out_us_ARMzNK4ApawIv34yHwGy4M 21.11.2014.

[33] Nilsson, A. (2012), Statistics of "450.000 leaked Yahoo accounts", http://pastebin.com/2D6bHGTa, 13 July 2012.

[34] Sanger, D., Shanker, T. (2014), N.S.A. Devises Radio Pathway Into Computers. The New York Times, 14.1.2014. http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?_r=0

[35] Schneier, B. (2005), Sony's DRM Rootkit: The Real Story, Schneier on Security blog, https://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html

[36] Schmidt A. (2013). The Estonian Cyberattacks, in: Healey J. (ed.), The fierce domain – conflicts in cyberspace 1986-2012, Atlantic Council, Washington, D.C., 2013. Online: http://netdefences.com/wp-content/uploads/SchmidtA-2013-Estonian-Cyberattacks.pdf

[37] Schmitt M. N. (ed.) (2013), Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press

[38] Storm, D. (2012), Pacemaker hacker says worm could possibly 'commit mass murder', in: ComputerWorld, http://blogs.computerworld.com/cybercrime-and-hacking/21163/pacemaker-hacker-says-worm-could-possibly-commit-mass-murder

[39] Tóth-Laufer, E., Takács, M., Rudas, I. (2013), Interactions Handling Between the Input Factors in Risk Level Calculation. In: Szakál, A. (ed.) Proceedings of the IEEE 11th International Symposium on Applied Machine Intelligence and Informatics (SAMI 2013). pp. 71-76. (ISBN:978-1-4673-5928-3)

[40] Websense (2011), It's no longer a question of 'if' but 'when'!, Websense Inc., http://click.websense-email.com/?ju=fe2d1572746406757210079&ls=fdf01078716c077d7713737d&m=fefc1177756502&l=fec117787c66057a&s=fe2111757c620c78761170&jb=ffcf14&t=

[41] Weitzenkorn, B. (2012), Bank of France's Accidental Hacker Acquitted, http://www.technewsdaily.com/8140-accidental-hacker-bank-france.html, 21 Sep. 2012.

[42] Whitney M. (2006), *The Pentagon's War on the Internet*, http://www.informationclearinghouse.info/article11901.htm