UNIVERZITA KARLOVA V PRAZE

FAKULTA SOCIÁLNÍCH VĚD

Institut mezinárodních studií

Mezinárodní teritoriální studia

THE INFLUENCE OF CYBER TERRORISM THREAT ON THE AMERICAN SECURITY POLICY

(VLIV KYBERNETICKÉHO TERORISMU NA AMERICKOU BEZPEČNOSTÍ POLITIKU)

DISERTAČNÍ PRÁCE

Ing. Tomáš Rezek

Praha, 10.3.2015

Autor práce: Ing. Tomáš Rezek

Vedoucí práce: doc. PhDr. Miloš Calda

Oponent práce:

Datum obhajoby:

Hodnocení:

P**rohlášení**

1. Prohlašuji, že jsem předkládanou práci zpracoval samostatně a použil jen uvedené prameny a literaturu.

2. Předkládaná práce nebyla využita k získání jiného nebo stejného akademického titulu.

3. Souhlasím s tím, aby práce byla zpřístupněna pro studijní a výzkumné účely.

V Praze dne …….. Ing. Tomáš Rezek

Poděkování

Chtěl bych využít této příležitosti a poděkovat svému školiteli docentu Caldovi za jeho odbornou pomoc a za jeho rady. Rovněž bych chtěl poděkovat své manželce a rodičům za jejich podporu při mém studiu.

I. Abstract (English)

The aim of this dissertation is to answer the question of whether the U.S. security policy is influenced by the threat of cyber terrorism. The dissertation is divided into chapters that can be regarded as steps in a logical reasoning process.

In the first chapter, cyber space is introduced and described to illustrate its importance and complexity. The next chapter analytically compares various definitions of terrorism, and partially rejects the initial hypothesis that cyber terrorism is not included in the general definition of terrorism. The following chapter statistically analyzes the available data on terrorist groups and terrorist attacks to empirically confirm the hypothesis that terrorism is still a real threat to American security. The analysis actually proves that the threat of terrorism has not decreased in relation to the number of terrorist groups. It also shows that the number of terrorist attacks against the U.S. targets has significantly decreased in the United States, while terrorist actions have been increasing constantly on a global level. The analysis shows that the success rate of terrorists attacks does not form a time series, and therefore each terrorist attack has to be examined individually to assess its success probability. The following analysis reviews the possibilities of terrorists obtaining weapons of mass destruction in comparison with the option of cyber attacks. This analysis is based on case studies which prove that cyber attacks have the potential of being even more destructive than conventional terrorist attacks in some cases. The findings show that terrorists would be more likely to rely on massive attacks, whereas other actors like state-supported groups of hackers would probably launch more sophisticated and well- targeted attacks. The next chapter assesses the current position of the U.S. in cyber space. The results show that different factors have to be considered in cyber space to determine the cyber capabilities of a particular state. The position of the U.S. is not so dominant in cyber space, based on the findings in this chapter. Finally, the last chapter analyzes important documents that have shaped American security policy related to cyber terrorism and cyber security. This analysis shows that cyber terrorism has been addressed in documents influencing American security policy since 1998, when terrorists were first identified as a possible source of cyber attacks.

In conclusion, the dissertation confirms that the threat of cyber terrorism is indeed influencing the U.S. security policy, but that cyber security is a more important issue. Further research should focus on the role of the state in ensuring cyber security, and on the qualitative aspects of any security measures that are implemented.

Key words: Cyber space, terrorism, U.S., USA, cyber security, virus, terrorist attack, critical infrastructure, homeland security, hacker.

II. Abstract (Czech)

Cílem této dizertační práce je odpovědět na otázku, zda americkou bezpečnostní politiku ovlivňuje hrozba kybernetického terorismu. Práce je rozdělena logicky návazných kapitol, jejichž závěry formulují konečnou odpověď.

Kybernetický prostor je popsán v první části, která se věnuje především jeho významu a komplexnosti. Následující kapitola srovnává několik definicí terorismu. Výsledky analýzy dokazují, že kybernetický terorismus spadá pod obecnou definici terorismu. Další kapitola statisticky analyzuje dostupná data o počtu teroristických skupin a teroristických útoků. Závěry empiricky potvrzují, že terorismus představuje i nadále skutečnou hrozbou pro americkou bezpečnost. Jedním z důvodů je i neklesající počet teroristických skupin. Navzdory tomu, že počet teroristických útoků ve Spojených státech klesl, na globální úrovní došlo k nárůstu teroristických akcí proti americkým cílům. Statistická analýza rovněž dokazuje, že úspěšnost teroristických útoků nelze považovat za časovou řadu, a tudíž je nutné vždy analyzovat pravděpodobnost úspěchu konkrétního útoku. Navazující kapitola zkoumá možnosti teroristů získat přístup ke zbraním hromadného ničení v porovnání s možnostmi, které představují kybernetické útoky. Případové studie v další kapitole dokazují, že kybernetické útoky mohou být v některých případech dokonce ničivější, než konvenční teroristické útoky. Výsledky naznačují, že teroristé budou spoléhat na masivní kybernetické útoky, zatímco státem podporované skupiny hackerů budou spíše schopné lépe cílených a sofistikovanějších útoků. Předposlední kapitola se věnuje pozici Spojených států v kybernetickém prostoru a ukazuje, že pozice Spojených států není ve virtuálním světě zdaleka tak suverénní, jako v reálném světě. Poslední kapitola analyzuje důležité dokumenty formující americkou bezpečnostní politiku z pohledu kybernetického terorismu a kybernetické bezpečnosti. Výsledky ukazují, že kybernetický terorismus se v těchto dokumentech objevuje již od roku 1998, kdy byli teroristé identifikování jako možní strůjci kybernetických útoků.

Tato dizertační práce dokazuje, že hrozba kybernetického terorismu ovlivňuje americkou bezpečnostní politiku, ale kybernetická bezpečnost je důležitějším tématem. Další výzkum by se měl soustředit na roli státu při zajišťování kybernetické bezpečnosti a na kvalitativní aspekt realizovaných bezpečnostních opatření.

Klíčová slova: Kybernetický prostor, terorismus, kybernetický terorismus, kybernetická bezpečnost, teroristický útok, kritická infrastruktura, hacker, národní bezpečnost, Spojené státy, Amerika.

III. List of abbreviations

CALEA	Communication Assistance for Law Enforcement Act
CERT	Computer Emergency Response Team
CI	Counter Intelligence
CI/KR	critical infrastructure and key resources
CIA	Central Intelligence Agency
CISA	Cyber Security Information Sharing Act
CISPA	Cyber Intelligence Sharing and Protection Act
CNCI	Comprehensive National Cyber Security Initiative
CRM	Customer Relationship Management
DCEO	Defensive Cyber Effects Operations
DDoS	Distributed Denial of Service attack
DHS	Department of Homeland Security
DoS	Denial of Service
ERP	Enterprise Resource Planning
EU	European Union
FBI	Federal Bureau of Investigations
FISMA	Federal Information Security Management Act of 2002
FLAG	Fiber-Optic Link Around the Globe
ICTs	Information and Communication Technologies
INSCOM	U.S. Intelligence and Security Command
ISO	International Organization for Standardization
ITU	International Telecommunication Union
LAN	Local Area Network
LoC	Lines of Code
NCIJTF	National Cyber Investigative Joint Task Force
NDCM	Nonintrusive Defensive Countermeasures
NETCOM	Network Enterprise Technology Command/9th Signal Command
NIPP	National Infrastructure Protection Plan
NIST	National Institute for Standards and Technology
NSA	National Security Agency
OCEO	Offensive Cyber Effects Operations
OMB	Office of Management and Budget
OSI model	Open System Interconnection model
R&D	Research and Development
SQL	Structured Querry Language
START	Study of Terrorism and Responses to Terrorism
STRATCOM	Strategic Command
TCP/IP	Transmission Control Protocol / Internet Control Protocol
U.S.	The United States
US-CERT	United States Computer Emergency Response Team
USSS	United States Secret Service

Content

1. Introduction

1.1. Opening

Inventions have always been the key to development. Thanks to great minds, mankind has made incredible progress in the 20th century. But every invention is accompanied by risks. The steam engine was a historical breakthrough in providing first power, and then later, locomotion. But many people died because of accidents, and thousands of others protested against steam engines fearing the loss of their jobs. Some two hundred years later, the first cars appeared - again, a great invention that mobilized the masses. Nevertheless, it required a new type of infrastructure and a special code of behavior on the roads. The speed of progress and innovation has multiplied and the technological gaps between successive generations are increasing. Many people say that this is mainly due to computers and to the evolution of information and communication technologies (ICTs), which have resulted in the emergence of cyber space as understood today. In the last 20 years, cyber space has become vital to a modern way of life. Modern world economies are becoming more and more dependent on cyber space and on ICTs. Not only do people need to cope with the changes cyber space has brought to everyday life, but also with the risks related to cyber space. Apart from the social and political challenges cyber space brings, there are security risks caused mainly by the increasing dependency on ICTs and on cyber space.

The world is changing, but remains full of differences. These differences - cultural, political, social, economic and other; were some of the causes that actually led to what some people call the "clash of civilizations."[1] Terrorism has become one of the main security threats in a large part of the world. Terrorist attacks cause fear and terror. They result in panic and their aim is to intimidate society. The attacks must be surprising and destructive; thus, cyber space is an ideal dimension for terrorists. There are almost no boundaries, and there are many possible targets in cyber space. So far, not a single cyber terrorist attack has happened, mainly due to the very ambiguous definition of cyber terrorism. But this does not mean that the risk does not exist. The fundamental question is whether western societies have used the last twenty years to create safety regulations,

[1] Samuel P. Huntington, *The Clash of Civilizations?,* (Simon&Schuster: New York, 1996)

to implement security measures and to educate their citizens, and thereby prepared themselves to face the cyber terrorism threat. Or maybe they have not.

1.2. Related discussion

The dissertation and related research reflects discussions about two main topics – the terrorism threat and increased usage of cyber space and modern technologies. Cyber terrorism is in the intersection of these two topics.

Terrorism has been regarded as a major threat to national security especially after the 9/11 attacks. New security policies have been implemented in reaction to these attacks. The attacks actually speeded up the creation of the Department of Homeland Security in the U.S. and triggered many changes in the existing security policies as well as changes in the legislation. The impact of the attacks was strong especially in the U.S., but it is possible to track the consequences in other western countries as well. Many countries suddenly introduced articles concerning terrorist attacks into their national security or foreign policies. These reactions were of course much stronger in nations that had suffered from terrorist attacks. Financial resources needed to support newly launched counter-terrorist activities were provided in abundance as the public opinion strongly supported this direction.

Nevertheless, the public support was not so unequivocal when individual privacy was violated in order to better protect citizens from terrorists. These voices in the U.S. during the period right after the attacks were often ignored or labeled as unpatriotic. The discussion about the appropriateness of counter-terrorist measures at the expense of civil liberties started in September 2001 when the U.S. Supreme Court Justice Sandra Day O'Connor pointed out to possible risks of the counter-terrorist campaign.[2] Other voices appeared later – Nadine Strossen, the president of American Civil Liberties Union[3], or Professor Laurie Thomas Lee.[4] Increased surveillance of public spaces or higher authority of counter-terrorist investigators can be taken as examples of problematic activities in conflict with civic rights. Critical voices increased in their

[2] Linda Greenhous, *O'Connor Foresees Limits on Freedom,* (New York Times, 2001), http://www.nytimes.com/2001/09/29/national/29SCOT.html (accessed on 21st February 2013)

[3] Nadine Strossen. *Terrorism's Toll on Civil Liberties*, (Haworth Press: USA, 2005), page 365 - 377

[4] Laurie Thomas Lee. *The USA PATRIOT Act and telecommunications: privacy under attack*. (Rutgers Computer & Technology Law Journal 29.2, 2003)

strength especially during the President Bush's second election term, for instance Joseph Margulies[5] or Glenn Greenwald.[6] The number of terrorist attacks committed in the U.S. was very low and exhausting conflicts in Iraq and Afghanistan were losing their momentum. The decrease of support to the ongoing war on terror was among other reasons that influenced the result of the Presidential elections in 2008.

The opposition to the legislative changes related to counter-terrorism activities introduced new arguments to support their cause. The very first argument that the increased security is in proportion to the "damage" done to civil rights and privacy mentioned by Justice O'Connor was joined by the argument that the threat of terrorism has been reduced, and therefore strong security measures violating civil rights are no longer necessary.[7]

Another argument is that since terrorism is an example of asymmetric conflict[8], the security can never be absolute as the attacker will always find the weak spot where to focus his activities. Moreover, security can be defined more like a process than a state. It has to be constantly updated to reflect the changes in the nature of the threat or in the environment. Rigid security system might not address the latest security issues and fail to prevent terrorist attacks. 9/11 attacks have brought more attention to terrorism also in the academic community. The threat of terrorism has been approached from various perspectives – political, social, economic and of course security. Some researchers focused on the future of terrorism, like Andrew M. Colarik,[9] Todd Sandler[10] or Brynjar Lia.[11] These included the use of weapons of mass destruction for terrorist attacks, transformation into political parties, deepened religious fundamentalism and also a spillover of terrorist activities in cyber space.

---

5 Joseph Margulies, *Guantanamo and the abuse of Presidential Power*, (Simon & Schuster: USA, 2006)
6 Glenn Greenwald, *How would a Patriot Act*, (Working Assets Publishing: USA, 2006)
7 E.g. John Mueller, and Mark G. Stewart, *Balancing the Risks, Benefits, and Costs of Homeland Security,* (Homeland Security Affairs, 2011), https://www.hsaj.org/articles/43 (accessed on 19th February 2013)
8 Ekaterina Stepanova, *Terrorism in asymmetrical conflict: ideological and structural aspects,* (Oxford University Press, 2008), http://books.sipri.org/files/RR/SIPRIRR23.pdf (accessed on 24th February 2013)
9 Andrew Colarik, *Cyber Terrorism: Political and Economic Implications,* (Idea Group Publishing: London, 2006)
10 Todd Sandler, *The Past and Future of Terrorism Research*, (CREATE, 2009), http://research.create.usc.edu/cgi/viewcontent.cgi?article=1123&context=nonpublished_reports (accessed on 27th February 2013)
11 Brynjar Lia, *Globalization and the Future of Terrorism*, (Routledge: USA, 2005)

Cyber space was experiencing the .com bubble burst in 2001, when the 9/11 attacks took place. Nevertheless, it still played an important role in the U.S. economy and society. The importance of cyber space has even more increased since then as the implementation of modern technologies spread to almost all aspects of economic and social life. This boom was accompanied by alarm voices warning before the vulnerability created by the dependency of modern technologies. The security risk was mentioned for instance in studies[12] written by Marshall Adams and Joe Weiss, in which the authors analyzed incidents in critical infrastructure related to cyber security. The risk itself was later reflected during the presidential elections in 2008 by both Republicans and Democrats.[13]

The security risk of cyber space dependency has dramatically evolved during the last thirty years together with the perception of cyber security. The beginning of the vulnerability can be traced to the moment when computers were given important tasks related to critical infrastructure or to the services provided by the state like calculation of pensions or social benefits calculation. At this point, some officials realized that the increased efficiency and cost savings come together with the risk of a computer mistake or a system failure.[14]

The mistakes were caused by wrong programming, lack of control mechanism or were simply caused by the operator. This risk was soon increased by the creation of computer viruses. It is possible to say that the security risk has increased together with the rapid implementation of modern technologies in almost all domains of activity. The usage of computers introduced new risk – computers can fail. This vulnerability was acknowledged on a large scale in the 90's thanks to the problem of Y2K.

The pessimists mobilized because of possible chaos that would start when the computers broke down unable to distinguish between the year 1900 and 2000.

---

[12] Marshall Abrams, Joe Weiss, *Bellingham, Washington DC, Control System Cyber Security Case Study*, (Mitre/NIST, 2007), Marshall Abrams, Joe Weiss, *Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia,* (Mitre/NIST, 2008),

[13] Tomas Rezek, *Přinese nový prezident Spojeným státům bezpečnější kyberprostor?,* (NATOAktual.cz, 2012), http://www.natoaktual.cz/prinese-novy-prezident-spojenym-statum-bezpecnejsi-kyberprostor-1dr-/na_analyzy.aspx?c=A120904_074755_na_analyzy_m02 (accessed on 4th September 2012)

[14] *S.1766 – Federal Computer Systems Protection Act,* (Washington, Congress, 1977), http://www.gao.gov/assets/100/98793.pdf (accessed 27th October 2014)

Society and order would be destroyed as the critical infrastructure stopped working and the computers became uncontrollable. Y2K problem received lot of attention especially in the U.S. during the President Clinton's administration. The hysteria about the Y2K problem had a positive effect – people realized the increasing dependency on modern technologies and on cyber space. This dependency without proper approach becomes a security risk that can have serious impact on the U.S. economy and national security.

Year 2000 passed without any major effect on computers or other systems. Critics emerged[15] in reaction to the large financial resources spent on Y2K problem in the U.S. by the Cabinet and actually discredited many reasonable studies calling for a better protection of cyber space. Cyber terrorism as a term appeared in official documents right after the 9/11 attacks, when the threat of terrorism was projected into almost all domains. Cyber crime has increased in size and complexity, so has the number of cyber attacks. However, not a single cyber attack has been officially recognized as an act of terrorism so far in the U.S. This leads to a question whether cyber terrorism is a real threat that needs to be defined and specially addressed.

But what is actually cyber terrorism? Journalist often use the term 'terrorism' for attacks that do not have the characteristics of the definition of terrorism to get more public attention. Moreover, the definition of terrorism differs across the world and even on the national level. The same ambiguity is valid also for the term 'cyber terrorism'. Nevertheless, the definition is very important. The academic debate is very often based on the applied definition.[16]

The term cyber terrorism is linguistically linked to terrorism. But can the definition of terrorism be applied also to cyber space? Cyber attacks might cause substantial damage, but this damage is almost always virtual in the first place. One of the important reasons for legal definition of terrorism is the authority given to security forces when dealing with terrorist suspects or terrorists. As already mentioned, the legislative changes introduced after 9/11 attacks enabled security forces dealing with terrorism to use

[15] E.g. OJR staff, *Post-Mortem: The Bug Appears to Be Beaten,* (USC, 2000), http://www.ojr.org/ojr/technology/1017966298.php (accessed on 16th February 2013)
[16] E.g. opinion of Thomas Rid, *Cyber War Will Not Take Place,* (Hurst&Company: London, 2013) on cyber war based on the assumption that war requires physical violence.

exceptional methods of investigation that might be regarded as illegal in "conventional" cases. Moreover, how has the terrorism threat changed? Because if the war on terrorism is successful, the threat itself should be reduced. If the premise that cyber terrorism is related to terrorism, than the decrease of the risk for terrorism should apply also to the cyber terrorist attacks. These are some of the questions raised in the dissertation.

2. Research question

The research question for the dissertation is formulated as follows: Is there evidence to recognize cyber terrorism as a threat to the U.S. security?

To be able to answer this question, it is necessary to analyze different but interlinked topics to formulate answers to more detailed questions that will lead to the conclusive answer to the research question.

The first question is: What is cyber terrorism? The term itself is composed of two components – cyber and terrorism.[17] Firstly, a brief introduction into the cyber space topic is given to better understand the main characteristics of this domain. Secondly, it is necessary to comprehend the definition of terrorism and to analyze if it is also applicable to cyber space. Once it is confirmed that cyber terrorism is actually terrorism in cyber space with all the aspects of the definition, it is possible to move to the next step.

The second step is focused on terrorists and their actions. It is necessary to confirm if terrorists pose still a threat to the U.S. security. If not and the threat of terrorism is decreasing, so should the threat of cyber terrorism. Question for this part is: Is terrorism still a threat to the U.S. security? Proving that terrorists are still active and present a security risk is a basis for the logical conclusion that terrorist may launch cyber attacks. However, it is necessary to provide more information to complete the deductive process to state that terrorists will use cyber attacks.

[17] There are various forms of the term cyber terrorism used in literature: cyber terrorism, cyber-terrorism or cyberterrorism. The same applies to the other terms like cyber space. Cyber terrorism is used in this thesis and in the dissertation.

The third question therefore is: Are terrorists forced to change their current tactics? Again, the yes answer is not sufficient alone. Terrorists may be forced to seek new tactics, but there are other options than cyber terrorism. Therefore it is needed to answer the question if terrorists are likely to prefer cyber attacks to other options. Four main areas are analyzed to find this answer – the tendency of terrorists to use cyber attacks, the destructive capability of cyber attacks, the position of the U.S. in the cyber space and the approach of the U.S. administration towards cyber terrorism.

The conclusive answer to the research question is formulated considering the findings from individual steps of the reasoning process. In general, the answer will be yes, if all discussed research steps confirm formulated hypothesis.

3. Current research of the topic

Cyber security and terrorism are two topics addressed in many publications from different perspectives. There is a vast number of publication addressing the technical aspects of cyber security. But these publications are intended for technical audiences, and they do not consider the implications of cyber security on international relations or national security.[18] The importance of cyber security and cyber space to national security is addressed in some publications, but very often from a legalistic point of view, or with little attention to cyber terrorism per se. There are some very interesting articles on the cyber terrorism problem,[19] but cyber terrorism is often described as a unique problem not related to the existing terrorism threat, and they fail to cite convincing cases showing the importance of cyber terrorism. Some authors analyze the role of government in the cyber security process,[20] but in these publications, cyber terrorism is just one possible threat to cyber security, and therefore is not analyzed in detail. There are many publications focusing on various aspects of terrorism – political, social, psychological, etc. However, such publications do not consider the possibility of cyber terrorism, or their approach reveals a lack of any fundamental knowledge of the cyber security problem.[21] On the other hand, some publications discuss the evolution of the society in relation to cyber space.[22] One publication takes an approach similar to that applied in this dissertation: the book "Cyber War"[23] by Richard A. Clarke, former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism. In this book, Clarke describes his concerns for national security in relation to cyber threats based on his unique experience. Still, the possibility of cyber terrorism is overshadowed by other important topics described in this book.

This dissertation is aimed to increase the small number of publications addressing the issue of cyber terrorism, while taking into consideration terrorism and national security. The argumentation used in this dissertation presents new facts supporting the

---

[18] For instance Anonymous, *Maximum Security: A Hacker's Guide to Protecting Your Computer Systems and Network,* (Sams: Indianapolis, 2002)
[19] For instance chapter 19 Cyber Terrorism: Menace or Myth? (Franklin D. Kramer et al, *Cyberpower and National Security,* (Potomac Books: Virginia, 2009), pages 437 – 464
[20] For instance Jovan Kurbalija, *An Introduction to Internet Governance*, (DiploFoundation: Geneva, 2014) or Myriam Dunn Cavelty, *Cyber-Security and Threat Politics,* (Routledge: New York, 2008)
[21] For instance Luis de la doret Ibanez, *Logika Terorismu,* (Academia : Praha, 2009)
[22] For instance Simon Pont, *Digital State,* (KoganPage: London, 2013)
[23] Richard A. Clarke, Robert K. Knake, *Cyber War*, (HarperCollins: New York, 2010)

importance of cyber terrorism as a serious threat to national security. The dissertation also provides an overview of relevant policies and other documents responding to this pressing issue. This will hopefully offer useful orientation for other researchers who approach the problem. This document will also attempt to contribute to the discussion on the definitions of basic terms such as terrorism and cyber terrorism.

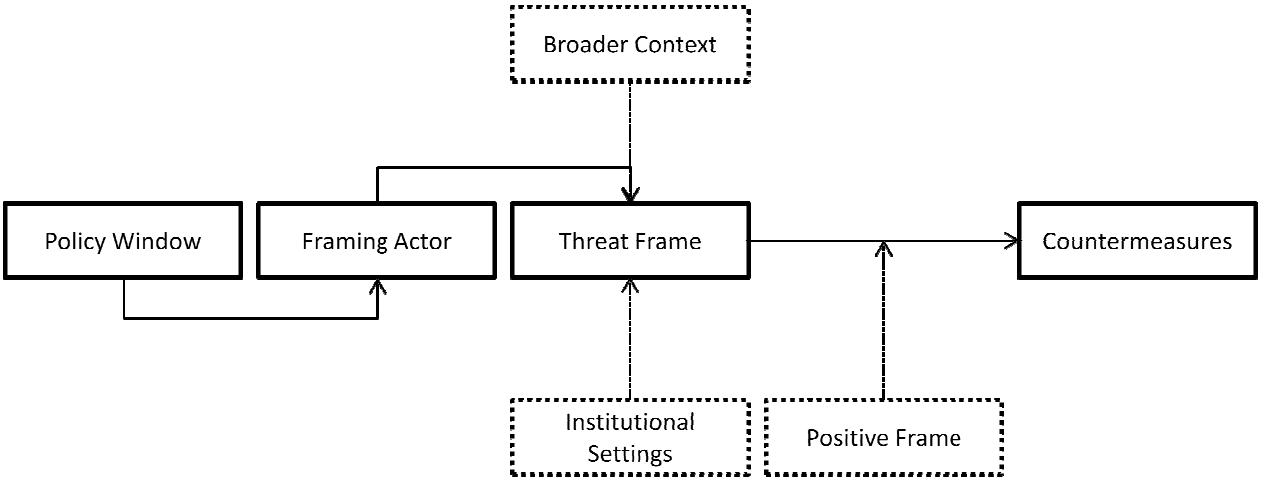
4. Methodology

4.1. Specification

This dissertation is focused mainly on American security policy. The reason is that the U.S. leads the ongoing war on terror, and the threat of terrorism remains very important to American security. Moreover, the U.S. is the birthplace of the Internet and many leading companies in the ICT industry were founded there. It is logical to expect that the implementation of modern technologies has reached a high level in the U.S. This means that the U.S. might be more vulnerable in cyber space, and therefore the issue of cyber security should receive more attention in its national security policy. Nevertheless, other countries are considered in particular chapters for comparison or for other analytical purposes.

4.2. Research approach

The research approach applied in the dissertation is derived from the framework for the study of threat politics applied by Myriam D. Cavelty.[24] The framework was used to analyze the process, how a topic becomes a security threat in an official document. The framework is based on four key variables and three influencing factors:



Picture 1- Schematic final framework by Myriam D. Cavelty[25]

Policy window may be initiated by a change in public opinion or by an increased attention of decision makers to a particular problem. Framing actors are usually security professionals or experts in the field who are able to formulate the threat or modify it. They share the same beliefs and have necessary resources. Threat frame is the

[24] Myriam D. Cavelty, *Cyber-Security and Threat Politics,* (Routledge: 2008, USA)
[25] Ibid, page 36

description of the threat. The threat frame therefore defines the security risks, suggests possible scenarios and contains necessary information to inspire supporters and motivate decision makers. Broader context is one of the three influencing factors. It can be current security situation on both national and international level, it may reflect the general public opinion or trends. Institutional settings are rules, norms or habits existing in the institutions involved in the national security protection and strategy. Positive frame symbolizes the resonance in opinions and beliefs of the framing actors, key decision makers and institutions. This resonance, if strong enough, materializes in the form of countermeasures. Countermeasures are not regarded in this framework as a simple consequence of the framing process, but rather as a variable indicating if the threat creation process is successful or not.

The framework presents an important logical process including key factors (variables) that are actually necessary to identify the threat. It serves as a guideline for the research in the dissertation. The variables are therefore analyzed in different chapters to find the evidence supporting or rejecting the hypothesis that cyber terrorism is a threat to the U.S. security.

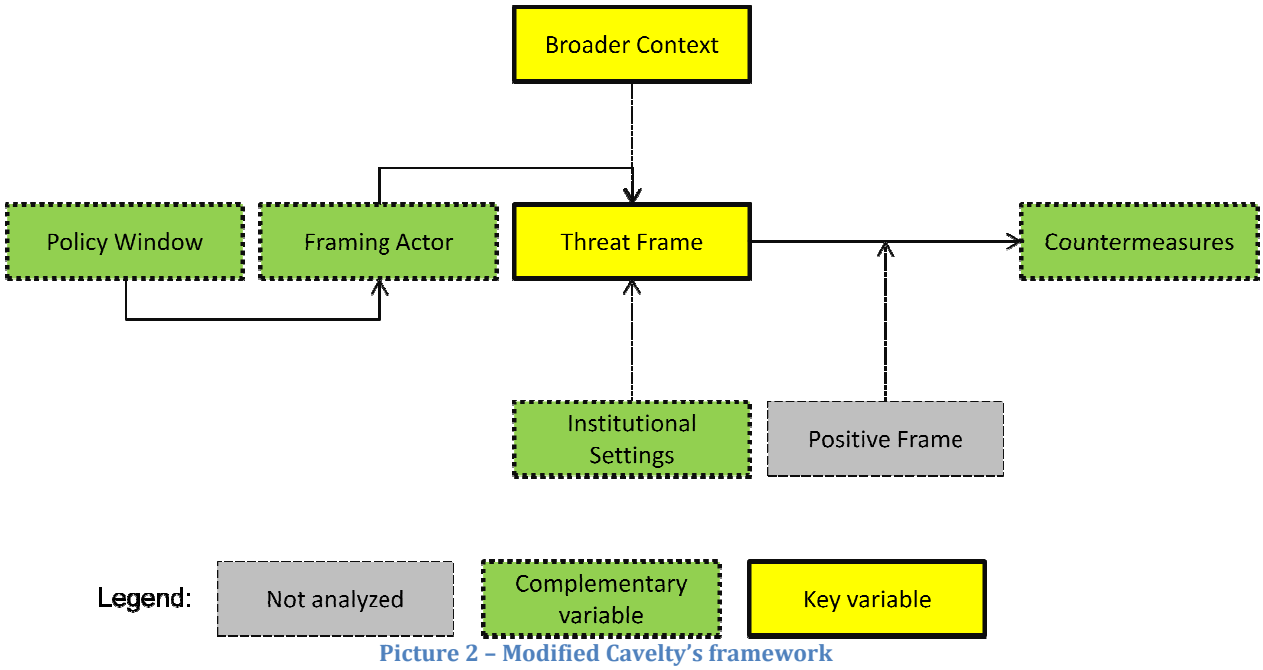
Policy window and Framing actor are related to actors, experts and stakeholders and to their perception of the problem or possible threat. Since the goal is to find real evidence, these variables are regarded as complementary in the analysis (chapter 10. Current position of the U.S. as a superpower in cyber space and chapter 11. American security policy). The reason is that these variables play important role in the definition of the threat, but they do not influence the existence of the threat itself.

On the other hand, Broader context and Threat Frame are variables that can be examined to find factual evidence to confirm or reject formulated hypothesis. Institutional Settings and Countermeasures are complementary variables, because the evidence collected in their analysis is not decisive. Existence of countermeasures or dedicated institution does not implicate that the threat is real. However, the analysis of these variables might provide important insight in the approach to the threat of cyber terrorism.

Broader context is approached from three perspectives – threat of terrorism to the U.S. (chapter 7. Terrorism – prevailing threat?), U.S. position in cyber space (chapter 10. Current position of the U.S. as a superpower in cyber space) and options for terrorists (chapter 8. Options for terrorists – cyber weapons or WMD?). Case studies are created to define Threat frame and to measure the possibilities terrorists might gain switching to cyber attacks (chapter 9. Cyber terrorism case studies). Institutional settings is included in the analysis of the U.S. position in the cyber space (chapter 10. Current position of the U.S. as a superpower in cyber space) and also in the analysis of important documents shaping the U.S. security policy (chapter 11. American security policy). Countermeasures are included in the analysis of important documents shaping the U.S. security policy (chapter 11. American security policy).

Positive frame variable is not analyzed, because in the context of this dissertation if it was sufficient and countermeasures were implemented, it is included in the analysis of Countermeasures variable. Otherwise it cannot bring any evidence usable for the analysis in this dissertation.

Following picture shows the Cavelty's framework modified for the purpose of the dissertation:



Picture 2 – Modified Cavelty's framework

4.3. Dissertation structure

The fifth chapter "What is cyber space and why it is so important" is a brief introduction into the phenomena of the Internet, cyber space and modern technologies. It describes the basic architecture of cyber space and its importance from various perspectives. It also displays the main aspects of cyber space that have to be considered when defining the term cyber terrorism.

The sixth chapter "Terrorism" is focused on the definition of terrorism and cyber terrorism. Different existing definitions are analyzed and compared. The analysis focuses on the attributes limiting the application of a given definition on the activities executed in cyber space. Apart from interesting comparison of various definitions of terrorism this chapter answers the fundamental question whether the definition of terrorism is applicable to cyber space and thus cyber terrorism is a subtype of terrorism.

The seventh chapter "Terrorism – prevailing threat" applies statistical methods on the database of terrorist attacks and terrorist groups to confirm the hypothesis that terrorism has remained as a serious threat to the U.S. security despite the ongoing war on terror.

The eighth chapter "Options for terrorists – cyber weapons or WMD?" compares different options available to terrorists presuming that they are forced or they need to change their current tactics. It also explains basic cyber security risks and dangers. Weapons of mass destruction are used as a benchmark for the comparison with cyber attacks. This chapter shows that cyber attacks are a very affordable option.

The ninth chapter "Cyber terrorism case studies" contains more than fifteen case studies describing real terrorist attacks or cyber security incidents. An alternative scenario in the form of a cyber attack or a physical attack is described for every case to provide data for basic analysis and comparison of cyber attacks and physical attacks considering several criteria. This chapter answers the question whether cyber attacks can be as destructive as "conventional" terrorist attacks using real examples.

The tenth chapter “Current position of the U.S. as a superpower in cyber space” offers a comparison of the U.S. position in cyber space with other states like China, Russia or North Korea. The comparison is based on three attributes – offensive capacities, defensive capacities and dependency on cyber space. This comparison provides important information about the institutional background in the U.S. regarding the cyber space and it also reveals if the U.S. is highly vulnerable in cyber space or not.

The eleventh chapter “American security policy” analyses key documents shaping the American security policy. Analysis in this chapter not only maps the evolution of the approach towards cyber attacks, cyber terrorism and cyber security, but it also serves as a supportive check if cyber terrorism is reflected in official documents or not.

The twelfth chapter “Conclusion” sums up the findings of the thesis and the answer to the research question.

5. What is cyber space and why it is so important

5.1. Definition of cyber space

The online version of the Oxford dictionary says: "Cyber space is the notional environment in which communication over computer networks occurs."[26] However, when saying cyber space many people will think only of the Internet. But cyber space is much larger. It also contains private networks of various companies (intranets), public databases administered by the state and other systems. Cyber space is everywhere where network communication occurs. Sometimes it is obvious. Sending an email from a smartphone is an action taking place in cyber space. But not everyone realizes that a modern refrigerator can join the network and send a message to the manufacturer about needed repair and therefore brings cyber space to other unexpected situations. The same counts for the traffic lights, tollgates, alarm clocks and for many other objects of everyday use. One of the reasons is that cyber space is used for communication and information sharing. It is possible to use "traditional" communication technologies, but in some cases it is more convenient to communicate in cyber space (e.g. the refrigerator). But cyber space plays more important roles. Cyber space gradually embraced important segments of social and economic interaction in the society. Social networks, online services, mobile phone applications, navigation systems and many other gadgets or programs became part of lifestyle in developed countries and vast majority of them uses or exists in cyber space. Cyber space is therefore not an artificial dimension used only by few experts or governmental systems; it plays an important role globally in the society. The dependency on cyber space is not any more a mere theory – developed societies depend heavily on the modern information technologies and on cyber space not only for storage of information but, also for the exchange of information, processing and automated reactions[27].

5.2. Size of cyber space

Size of cyber space largely depends on the chosen metric. Moreover cyber space is also made up by infinite number of networks, hardware and systems. It is impossible to collect complete information on a global level to precisely state the result; mainly

[26] Oxford Dictionary, http://www.oxforddictionaries.com/definition/english/cyber space (accessed on 21st January 2013)
[27] Myriam Dunn Cavelty, *Cyber Security and threat politics*, (Abingdon: Routledge, 2007), page 19

because relevant statistics are so numerous and cannot be accessed in a coherent manner, but also because some of the statistics are classified (e.g. for military networks). Therefore some publications and researchers focus on the Internet to demonstrate the size of cyber space. But the size itself is not important. It simply illustrates the usage of cyber space and the influence it has. The usage of cyber space and of modern technologies can create dependencies that may evolve in potential security risks related to cyber space.

5.2.1. Internet users

One of the measures used to define the size of the Internet is the number of users. Nevertheless, the total number of Internet users would have to use all national statistics. Due to possible differences in methodology and definitions, official statistics from various sources significantly differ. For instance, Gartner study[28] concerning data storage published in 2013 mentions 1.7 billion Internet users, but the CIA Factbook[29] states 2.1 billion users based on data from 2010. Internet statistical website[30] states that the number of Internet users based on data from 2012 is 2.4 billion. Recent data published by International Telecommunication Union (ITU) says[31] that the number of individuals using the Internet is over 2.7 billion. The estimated number of users for 2014 is almost 3 billion. Following chart describes the increasing share of internet users form the developing world:

[28] John Monroe, *Forecast Analysis: Hard-Disk Drives, Worldwide*, (The Gartner, 2013), page 8, http://www.gartner.com%2Fdoc%2F2583019%2Fforecast-analysis-harddisk-drives-worldwide&ei=_gFxVMCsNoj1OM3CgNAD&usg=AFQjCNF0RhW9ZrhAfP-6S9xu4iohi_2OwA&bvm=bv.80185997,d.ZWU (accessed on 9th September 2013)

[29] Central Intelligence Agency, *The World Factbook* 2013-14 (Washington DC, CIA, 2013), https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html (accessed 12th April 2014)

[30] "Internet World Stats 2012" , Internet and world stats – usage and population statistics, http://www.internetworldstats.com/stats.htm (accessed on 3rd April 2013)

[31] "Key ICT indicators for developed and developing countries and the world (totals and penetration rates)", ITU World Telecommunication/ICT Indicators database, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/ITU_Key_2005-2014_ICT_data.xls (accessed on 6th May 2014)

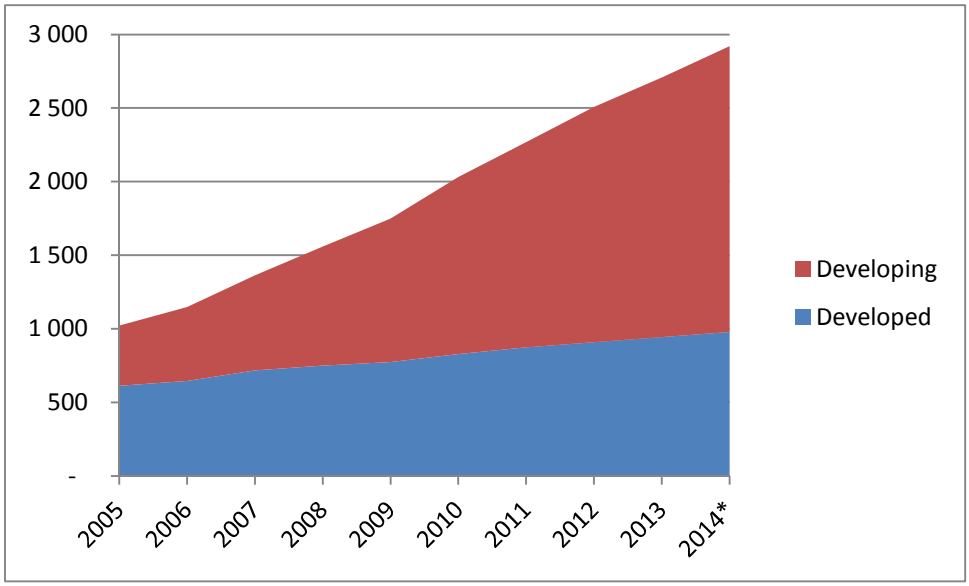


Chart 1 – Number of individuals using the internet, based on ITU data

China and other countries are using the increasing share of internet users from the developing world as an argument to get more influence over the Internet governance compared to current status.[32] To support their stand representatives from developing countries refer to the fact that the Internet coverage in the developing world is still much lower than in the developed world. The following chart shows the percentage of individuals using the Internet in the developed and developing world together with the estimation for the year 2014.

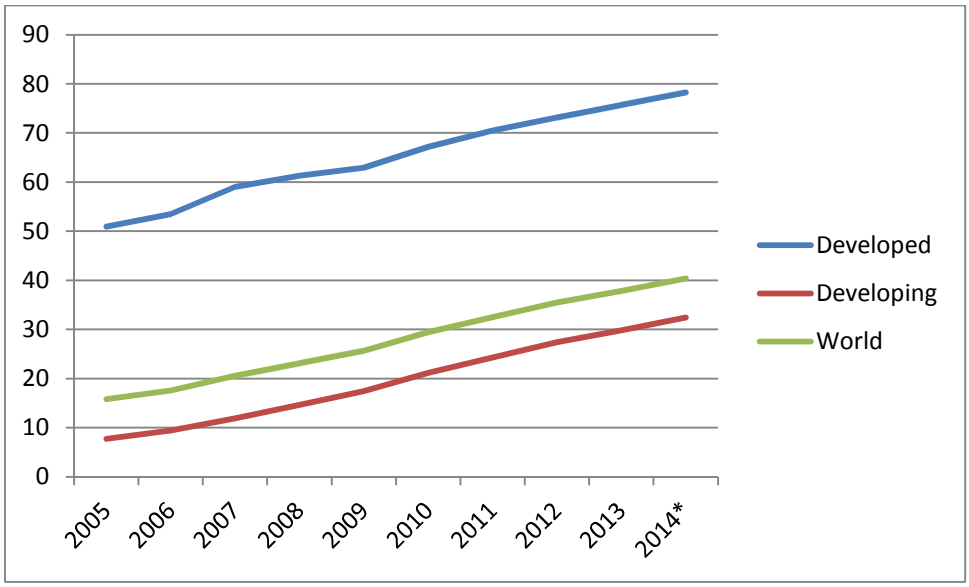


Chart 2 - Percentage of individuals using the Internet in the developed and developing world, based on ITU data

[32] Discussed during Sino-European Cyber Dialogue, 31st March – 1st April 2013 (Genève, Switzerland)

The percentage of internet users in developing world is less than half of the percentage in the developed world, but in the numbers the developing world has already twice as much internet users as the developed world. Experts agree that the number of internet users will continue to increase. Cisco analysis[33] forecasts that by 2017, there will be over 3.7 billion Internet users. In that time three from four Internet users will be from the developing world.

5.2.2. Data size

The amount of information accessible in cyber space is immense, but how to measure it to be more precise? Instead of measuring the size of information stored in cyber space, it is possible to consider total manufactured storage space. The following chart displays the evolution of hard disks manufacturing market based on the Gartner study.

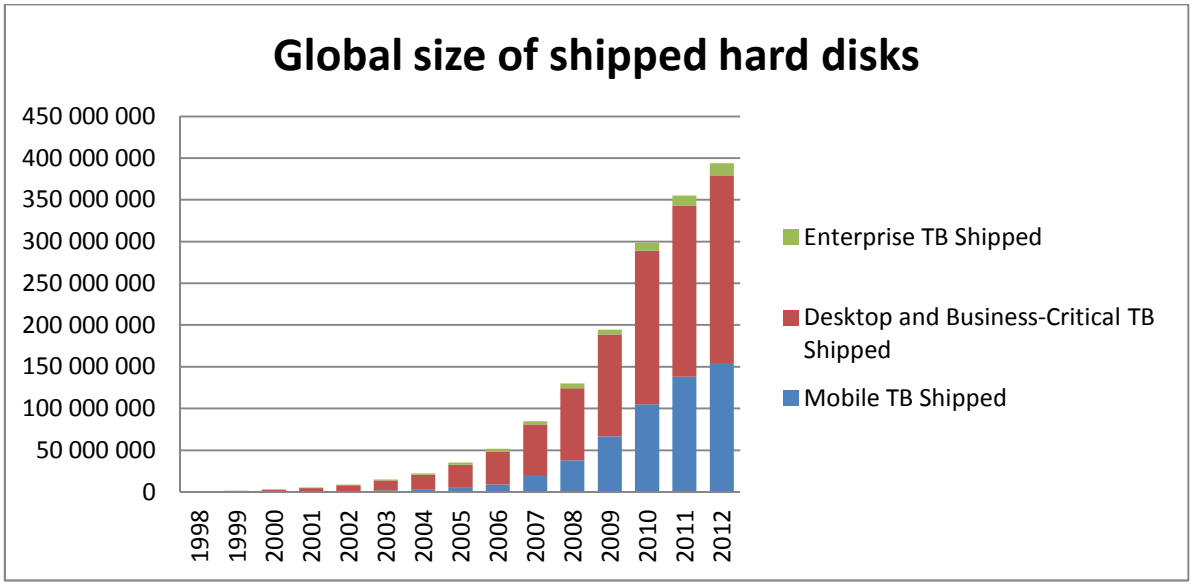


Chart 3 – Global size of shipped hard disks, based on Gartner study[34]

Of course not all hard disks are used to their full capacity, but this is compensated by the fact that cumulativeness of the storage space over the years is not considered. The fact that not all hard disks might be a part of cyber space cannot put the growing tendency in doubt.

---

[33] Cisco Press Release, *Cisco's Visual Networking Index Forecast Projects Nearly Half the World's Population Will Be Connected to the Internet by 2017*, (Cisco: California, 2013), http://newsroom.cisco.com/release/1197391/ (accessed on 9th June 2013)

[34] John Monroe, *Forecast Analysis: Hard-Disk Drives, Worldwide*, (Gartner, 2013), page 8

It is very difficult and inaccurate to compare the size of information stored in cyber space with other media. Nevertheless, the dominancy of cyber space can be demonstrated by the study "How much information?" conducted in 2003 at Berkeley University[35]. It says that the amount of information produced on paper in 2003 was slightly over 1 000 000 TB. The size of shipped storage space in the same year was already five times larger (5 226 596 TB). These numbers are still very small when compared to nowadays data production. eBay stores incredibly large amount of data, not only about the goods and related transaction, but also metadata and other big data for further analysis about users' behavior or browsing history. eBay in total needs to store more than 200 TB of new data every day.[36]

But what is more important than the size of information stored in cyber space is the possibility to efficiently search for needed information. Thanks to search engines and specialized software designed to work with large databases, the efficiency is much higher than with any other media.

5.3. Importance of cyber space

Despite the difficulties when assessing the size of cyber space, it is even more difficult to state its importance. Obviously, everyone knows that cyber space is important because of all the service it provides and enables. But with regards to the cyber security, how difficult would it be to get by without it? Opinions differ – some say only minutes, others say human kind does not need this virtual dimension. Let us have a look at the importance of cyber space from various perspectives to better understand the threat cyber terrorism presents.

5.3.1. Social and educational aspects

Social aspects of cyber space depend on its current characteristics. In general, information and data stored in cyber space may be shared on the global level despite the fact that certain countries decided to exercise control over the data and information accessible via their national networks. In combination with the advancement in

[35] Peter Lyman, Hal R. Varian, *How Much Information*, (University of California at Berkeley: California, 2003), page 4, http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/printable_report.pdf/ (accessed on 29th June 2013)

[36] Tom Fastner, a Senior Member of the Technical Staff and an Architect with eBay, Teradata CTO Roadshow (Silicon Valley, 23rd June 2014), presentation on Teradata solution for eBay

computing, cyber space has huge impact on education. Since all the information is accessible globally and also created on the global level, it is much easier than before to find needed information. Let's take simple search of the size of population as an example. Some sixty years ago, the only option for ordinary student was to open the encyclopedia and find the number. But even if the book was published the same year, the statistics might have been several years old. There were also specialized magazines which might have contained more precise information, but they were not accessible globally. Approximately 40 years ago, the student might have called to a specialized office to get an answer, but usually he could only hope that the operator had better information than he could find. When first network connected American universities, it was the beginning of a new age. When the network was large enough and the data were regularly updated, students at main universities could search for needed data from specialized magazines uploaded to the network on a global level. Nowadays, it is possible to use online encyclopedia with latest data and verify the results with data from the online version of respected magazine. Of course, that in this case the importance of cyber space depends on the access to cyber space and on the created and updated content accessible online. The content again depends on the number of users willing to upload and share the information. Surprisingly, the qualification of the users creating the content is not the decisive factor. This was proved by the Wikipedia case, where the content created by ordinary users exceeded the content created by experts. The Wikipedia story illustrates the power of the networked society.

Wikipedia began as a complementary project for Nupedia (founded in 2000), a free online English-language encyclopedia project whose articles were written by experts and reviewed under a formal process. Wikipedia was originally designed to serve as "a feeder" for Nupedia. Mailing lists were created and invited people to create the content on the Wikipedia, which should be checked and transferred to Nupedia later. Wikipedia was launched in 2001. Wikipedia gained early contributors from Nupedia, Slashdot postings, and web search engine indexing. On August 8, 2001, Wikipedia had over 8,000 articles. On September 25, 2001, Wikipedia had over 13,000 articles. And by the end of 2001 it had grown to approximately 20,000 articles and 18 language editions. By late 2002, it had reached 26 language editions, 46 by the end of 2003, and 161 by the final days of 2004. Nupedia and Wikipedia coexisted until the former servers were taken

down permanently in 2003, and its text was incorporated into Wikipedia. English Wikipedia passed the mark of two million articles on September 9, 2007, making it the largest encyclopedia ever assembled, surpassing even the 1407 Yongle Encyclopedia, which had held the record for 600 years.[37] Project Nupedia was terminated in 2003 with approximately 100 articles.[38]

Access to the information on global level also increases the general awareness. It was said that the telegraph network reduced the geographical distance, but cyber space removed the borders and concentrated the world in one point. Modern technologies dramatically changed journalism. The public demands fresh information and in an online world this means minutes, hours in maximum. Paper media found themselves in a difficult position to pursue basic principles of journalism and in the same time to provide new information practically immediately and in pictures to attract the attention of the public. It is possible to argue if the quality of the information provided by online media is better or worse than in paper media twenty years ago, but it is indisputable much faster. The number of people relying on information from online media is increasing. Together with the television online news are the main sources of information in the Western world. A study published by Pew Research Center in 2012 shows that in the U.S., online media became the second most used media as a source of information right after TV. 55% of respondents watched TV previous day, while 39% of respondents went online to find the news. Only 29% of respondents read newspapers, while 33% listened to the radio.[39] Online media played important role in the increase in awareness. But it also helped to increase the amount of available information so much that it is more difficult for people to assess the information.

Cyber space is also a new dimension where social interaction takes place. Social networks are the place where the new generation lives - share opinions, exchange ideas and form relationships. Study published by Pew Research Center reveals that more than

[37] "Wikipedia", Wikipedia, http://en.wikipedia.org/wiki/Wikipedia (accessed on 13th January 2012)
[38] "Nupedia", Wikipedia, http://en.wikipedia.org/wiki/Nupedia (accessed on 13th January 2012)
[39] Andrew Kohut et al., *In Changing News Landscape, Even Television is Vulnerable*, (The Pew Research Center: Washington DC, 2012) page 3, http://www.people-press.org/files/legacy-pdf/2012%20News%20Consumption%20Report.pdf (accessed on 6th February 2013)

73% of online adult users use social networking sites.[40] It is true that the cyber dimension changes the behavior in some way, but this does not question the fact that cyber space plays an important role in the social lives as well.

5.3.2. Economic aspects

The economic aspect of cyber space can be analyzed from two perspectives – cost reduction and revenue generation.

The development of information and communication technologies (ICTs) and cyber space enabled significant cost reduction via increase in efficiency of internal processes. Modern systems implemented in companies have helped at first to increase profit margins, later to find reserves in increasingly competitive environment. Customer relationship management systems (CRM), enterprise resource planning systems (ERP), supply chain management systems and other systems enabled costs savings firstly in larger companies, but given the decrease of prices for needed software and hardware equipment, more companies might benefit from increased efficiency. Business intelligence solutions and developed analytics models enabled companies to fully capitalize their data and to increase the efficiency in marketing campaigns or in collections. Increased use of computers and specialized software also reduced employee related costs in certain industries, partly thanks to increased work efficiency and partly by reducing the optimal size of workforce. The possibility to communicate directly with possible business partners over cyber space without the need of middle man reduced the purchasing costs and increased the size of the market. Truly global market for companies is currently not the question of communication or purchasing, but it largely depends on logistic and delivery.

On the other hand, rapid development of cyber space and ICTs created a brand new industry. Number of consulting companies specialized in the ICTs stabilized during the economic crisis and after the .com boom, but the value of their business has not stopped

[40] Maeve Duggan, Aaron Smith, *Social Media Update 2013*, (The Pew Research Center: Washington DC, 2014), page 4, http://www.pewinternet.org/files/2013/12/PIP_Social-Networking-2013.pdf (accessed on 29th June 2014)

increasing.[41] Nowadays, cyber space enables communication on a truly global level. In combination with lower transportation costs this resulted on creating a global market in certain industries, where the distance between business parties is not a crucial factor. The success of electronic commerce largely depends on the computer literacy of the population and also on the confidence in the electronic business model – belief in the fact that the customer will receive the goods he or she ordered and paid for. And if not, that he or she will be able to get justice. The existence of cyber space also enabled the creation of completely new services, for instance, the online computer games industry or online marketing. It is true that the share of ICTs related industries on the GDP differs country from country, but the overall economic benefit of ICTs and cyber space cannot be overseen any more, especially in times of economic crisis and stagnation, especially when the direct relation between the Internet connectivity and GDP growth is used as a fact. For instance, 10% increase in broadband penetration could result in the increase in GDP by 1.38% in low and middle income countries according to white paper on economic impact of the ICT sector published by Net!Works[42]. On the other hand, study published by Ericsson in 2013[43] suggests that doubling broadband speed can add 0.3 GDP. The influence is in general undisputed, but the size of the effect is different. Following table published in ITU study[44] in 2012 presents different approaches to the quantification of this effect:

[41] Net!Works, *Economic impact of the ICT sector*, (Net!Works, 2012), page 5, http://www.networks-etp.eu/fileadmin/user_upload/Publications/Position_White_Papers/Net_Works_White_Paper_on_economic_impact_final.pdf (accessed on 18th September 2013)
[42] ibid, page 11
[43] Ericsson, *Analyzing the effect of broadband on GDP,* (Ericsson, 2013), page 1, http://www.ericsson.com/res/thecompany/docs/corporate-responsibility/2013/socioeconomic-effect-of-broadband-speed.pdf (accessed on 21st February 2014)
[44] Raul Katz, *The Impact of Broadband on the Economy: Research to Date and Policy Issues*, (Columbia: ITU, 2012), page 58, http://www.itu.int/ITU-D/treg/broadband/ITU-BB-Reports_Impact-of-Broadband-on-the-Economy.pdf (accessed on 25th April 2014)

Country	Authors – Institution	Data	Effect
United States	Crandall et al. (2007) – Brookings Institution	48 States of US for the period 2003-2005	Not statistically significant results
	Thompson and Garbacz (2008) – Ohio University	46 US States during the period 2001-2005	A 10% increase in broadband penetration is associated with 3.6% increase in efficiency
OECD	Czernich et al. (2009) – University of Munich	25 OECD countries between 1996 and 2007	A 10% increase in broadband penetration raises per-capita GDP growth by 0.9-1.5 percentage points
	Koutroumpis (2009) – Imperial College	2002-2007 for 22 OECD countries	An increase in broadband penetration of 10% yields 0.25% increase in GDP growth
High Income Economies	Qiang et al. (2009) – World Bank	1980-2002 for 66 high income countries	10% increase in broadband penetration yielded an additional 1.21 percentage points of GDP growth
Low & Middle income economies	Qiang et al. (2009) – World Bank	1980-2002 for the remaining 120 countries (low and middle income)	10 % increase in broadband penetration yielded an additional 1.38 in GDP growth

Table 1 – Research results of broadband impact on GDP growth by ITU

Despite the discrepancies in the results, the studies confirmed that there is a positive effect of internet connection capacity increase in the economic growth. Apart from the direct influence on the GDP through investments into necessary infrastructure, there are the benefits of job creation, education and increased effectiveness.

5.3.3. Political aspects

From the internal perspective, cyber space offers new opportunities for interaction between state and citizens. Many processes might be simplified by using ICTs, for instance online elections or personal agenda like changing address. On the other hand cyber space and its borderless content might be perceived as a potential threat. This lead to a tendency described by Gartner researchers[45] as a tendency to control. This tendency results in the increase of communication surveillance, monitoring of cyber space traffic and attempts to gain the capability to control the connection to the Internet on a national level. Using modern ICTs in critical infrastructure facilitates the management, but also introduces new security risks.

From the perspective of foreign relations, cyber space is a new domain for international interaction. Appropriate state departments have to address foreign companies operating via Internet on national markets and address any potential disputes. On a higher level, there are more important negotiations going on, for instance about international cooperation in fighting cyber crime or tracking hackers. In some cases cyber space might become a tool in foreign policy; for instance the speech of American ministry of foreign affairs Hillary Clinton,[46] in which she established the link between the free access to the Internet and freedom itself. This speech was a reaction to attempts of Egyptian government to switch of the access to the Internet in Egypt.

---

[45] Stephen Prentice, *The Future of the Internet: The Three Forces Shaping the Internet and How They Will Affect Your Business,* (The Gartner, 2012), page 3, http://www.gartner.com%2Fdoc%2F2118015%2Ffuture-internet-forces-shaping-internet&ei=3QJxVNe2F4ffPfS1gOgB&usg=AFQjCNG-Tunf76RI46LkrJRKXf2eby1_Ew&bvm=bv.80185997,d.ZWU (accessed on 17th October 2013)

[46] Hillary Clinton, *Remarks on Internet Freedom*, (2010), http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm (accessed on 24th November 2011)

The perception of the Internet and cyber space as a potential threat to the national security is reflected in national strategies across the world in many different ways – filtering content, blocking access or supervision of users' activities. These discrepancies are the reason for ongoing discussion on the Internet governance particularly between the representatives of developing and developed states.

5.3.4. Military aspects

The military aspect of cyber space was at the beginning only informational – connected computers and systems might contain militarily important data. However, the situation substantially changed when the number of users and subjects active in cyber space massively increased. Probably the first proof of a change in the military attitude on cyber space is the propaganda. Sending emails is much more effective than dropping leaflets. Emails were used to encourage Iraqi officers to surrender in 2003.[47] However, this usage of cyber space is just a new dimension to existing propaganda activities. The same counts for military intelligence trying to find important information in cyber space as well as in the real world. More advanced usage of cyber space and modern technologies for the military purposes are the crucial moment when the army fully embraced this domain. Modern military equipment practically depends on the modern technologies and on cyber space. Radars, tanks, jet fighters, night vision systems, all these things are either controlled by computers or connected to cyber space. Advanced technologies made the way for new weapons as well. For instance new drones or older ballistic missiles would not exist without technologies and systems that are also a part of cyber space. The development of cyber space as a new warfare dimension is highlighted by the existence of specially trained units dedicated to cyber attacks and to cyber war.

The strategic importance of cyber space is highlighted by the fact that many countries pursue offensive military programs focused on the exploitation of cyber space (for instance Netherlands). The usage of cyber space for military purposes can be traced during the conflicts in Georgia and Ossetia.[48] The operations included not only online

[47] Bret Baier and Liza Porteus, *Thousands of Iraqui Troops Appear Ready to Surrender,* (Fox News, 2003), http://www.foxnews.com/story/2003/03/19/thousands-iraqi-troops-appear-ready-to-surrender/ (accessed on 21st March 2013)

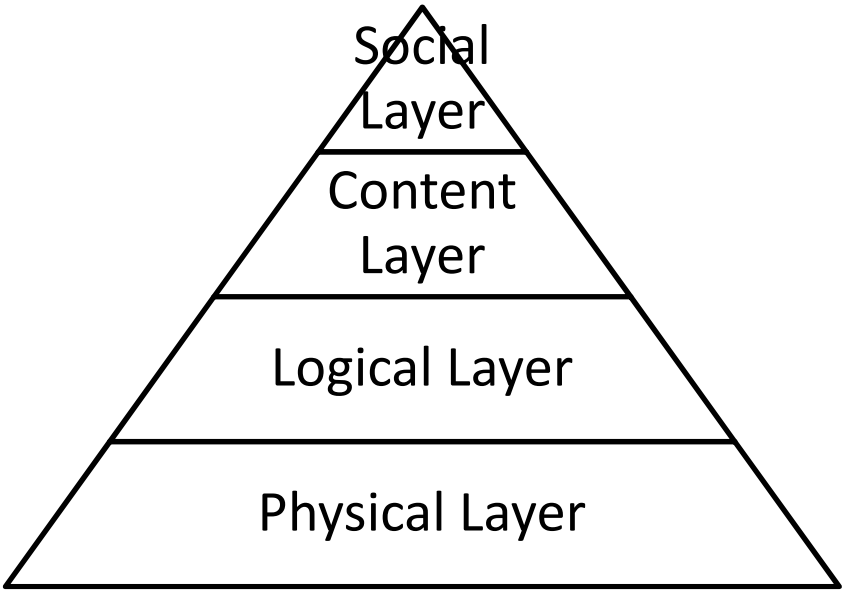
[48] Tom Espiner, *Georgia accuses Russia of coordinated cyberattack,* (cnet, 2008), http://www.cnet.com/news/georgia-accuses-russia-of-coordinated-cyberattack/ (accessed on 20th March 2013), AFCEA, *The Russo-Georgian War 2008: The Role of the cyber attacks in the conflict,* (AFCEA, 2012),

propaganda, but groups of hackers attacked online news portals and other important targets in the country. Different type of cyber tool was presumably used by Israeli forces during an air raid against Iranian nuclear facility.[49] The Israelis managed to fool radars monitoring the air space over Iran and hide the jets executing the attack.

Recent events in Ukraine showed that practically all military operations have their cyber side. These activities currently focus mainly on propaganda and disinformation, but the possibilities are much broader.

5.4. Different layers in cyber space

Despite the fact that different aspects of cyber space including some of the definitions have been briefly discussed, the complexity of this manmade domain needs another approach for better illustration. The four layer method introduced by David Clark[50] describes different aspects of cyber space. This model describes four different levels that make cyber space. Each layer is dependent on the previous layer in this model.



Picture 3 – Four layer model of cyber space by David Clark

http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf (accessed on 20th March 2013)

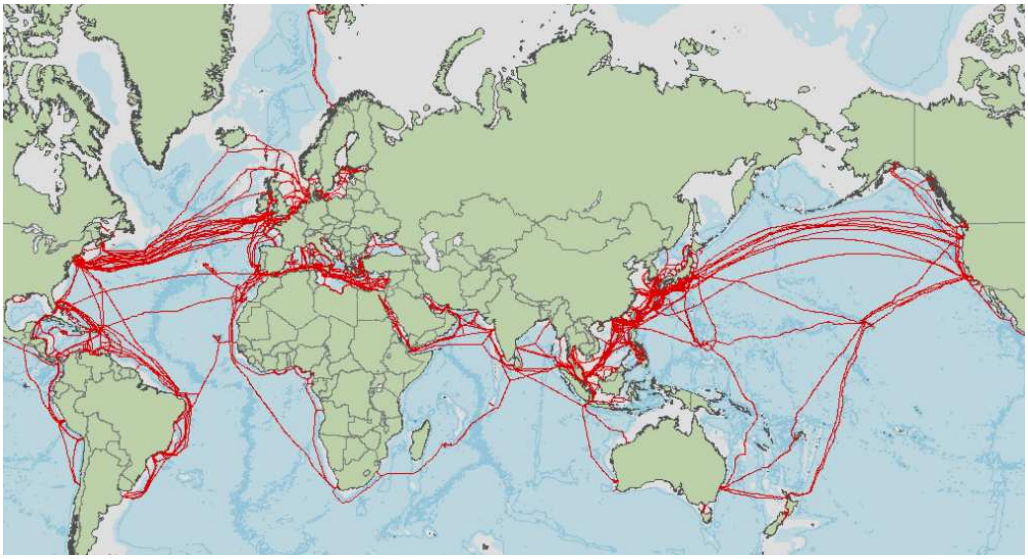
[49] Richard A.Clarke, Robert K.Knake, *Cyber War* (New York: HarperCollins Publishers, 2010), page 6

[50] David Clark, *Characterizing Cyberspace: Past, Present and Future*, (MIT/CAIL 2010), pages 2-4, https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyber space_1-2r.pdf (accessed on 18th July 2013)

5.4.1. Physical layer

This layer is the only layer related to cyber space existing in the real world. It covers all the hardware necessary for the exchange of information. In contains both wired and wireless devices. It is created by routers, servers, satellites, optical cables and other devices.

Let's consider the Fiber-Optic Link Around the Globe (FLAG) as an example. It is owned by Global Cloud Xchange and it is the largest private undersea system of more than 67 000 km of cables combined with fiber-optic cables on the land of the length of 200 000 km.[51] This system is regarded as a part of the Internet infrastructure backbone enabling connection to the Internet to many countries and territories.



Picture 4 – Undersea fiber-optic cables, Hong Kong Polytechnic University[52]

The importance of the physical layer and of the FLAG can be described through incidents damaging the undersea cables. Hengchun earthquake in 2006 caused damage to several of the submarine cables resulting in disruption of Internet services in Asia, mainly in Taiwan.[53] Another significant disruption of Internet services occurred in 2008 in the Middle East and India, when two undersea cables were damaged in the Mediterranean

[51] "The leader in global business communications", Global Cloud Xchange, http://www.relianceglobalcom.com/about-us.html (accessed on 26th August 2013)
[52] "Communications - the Future is Now", Hong Kong Polytechnic University, http://www.alanptlau.com/Research.html (accessed on 2nd July 2013)
[53] Brad Reed, *Internet cable cuts raise alarms over infrastructure vulnerabilities*, (NetworkWorld, 2008), http://www.networkworld.com/article/2282941/lan-wan/internet-cable-cuts-raise-alarms-over-infrastructure-vulnerabilities.html (accessed on 19th November 2013)

Sea, presumably by an anchor.[54] High speed Internet connection was turned off in East Africa in 2012 as an anchor disrupted the submarine cables close to Kenya.[55] Armenia, parts of Georgia and Azerbaijan were cut off the Internet in 2011 when a 75-year-old woman cut the fiber-optic cable while collecting metals for scrap yard.[56]

5.4.2. Logical layer

Logical layer refers to the software and to the protocols used within the software for particular reasons. This layer covers the code. Whereas software is easy to comprehend, the protocols are more difficult to understand even if they are crucial for the existence of the Internet as known today. Network protocol defines a set of rules or conventions for communication between devices in the same network. These protocols in general include mechanisms for devices to identify and make connection with each other; rules for data packaging into messages and rules for the transfer itself. Related network protocols are organized into families, for instance OSI model or TCP/IP.[57]

The Open System Interconnection model (OSI model) was introduced in 1984 by the International Organization for Standardization (ISO). The model can be identified as ISO/IEC 7498-1. The aim of the model was to explain and define the communication pattern between computers. Common understanding and the usage of the same definitions and processes enabled the development of communication all over the world since the same protocols were used on both communication sides. The OSI model divides the communication process into 7 layers. Every layer has a different function within the process of data exchange, as shows the following table:

---

54 BBC, *Severed cables disrupt internet,* (BBC, 2008), http://news.bbc.co.uk/2/hi/technology/7218008.stm (accessed on 13th March 2013)

55 BBC, *Ship's anchor slows down East African web connection,* (BBC, 2012), http://www.bbc.co.uk/news/world-africa-17179544 (accessed on 23rd June 2013)

56 Vaclav Nyvlt, *Důchodkyně šla "na dřevo", pilkou odřízla dva státy od internet,* (technet.cz, 2011), http://technet.idnes.cz/duchodkyne-sla-na-drevo-pilkou-odrizla-dva-staty-od-internetu-p61-/sw_internet.aspx?c=A110411_092852_sw_internet_nyv (accessed on 16th July 2013)

57 Mitchell Bradley, *Protocol (Network),* (About technology, 2010), http://compnetworking.about.com/od/networkprotocols/g/protocols.htm (accessed on 17th September 2013)

OSI model			
Layer number	**Layer name**	**Layer description**	**TCP/IP equivalent layer**
7	Application	Applications and services run on it, enables human network to interface the underlying data network	Application
6	Presentation	Coding and conversion of application layer data to ensure that data from the source device can be interpreted by the appropriate application on the destination device	
5	Session	Functions at this layer create and maintain dialogs between source and destination applications	
4	Transport	Tracking the individual communication between applications on the source and destination hosts	Transport
3	Network	Gives headers to the packets, opens the packets and checks the destination correctness	Internet
2	Data link	Creates data packets for transmission, controls access to the physical media	Subnet / Network access
1	Physical	The role of the Physical layer is to encode the binary digits that represent Data Link layer frames into signals and to transmit and receive these signals across the physical media that connect network devices	

Table 2 – Overview of OSI data layers based on presentation made at Goldsmith Department of Computing[58]

Transmission Control Protocol / Internet Protocol (TCP/IP) are two network protocols used together. TCP provides reliable, structured and error-checked transmission of information between programs running on computers connected through a network (e.g. LAN or Internet). IP defines packet structure that encapsulates the data. This "header" is then used in the addressing process to deliver the packet to the right receiver based on the IP address. TCP corresponds to the OSI layer 4 and IP to OSI layer 3. These two protocols gave the name to the TCP/IP model. This model was originally developed by DARPA as a part of ARPANET project and uses 4 layers.

[58] "Layering in Networked Computing", Goldsmiths Department of Computing, University of London, http://doc.gold.ac.uk/~mas01lo/Teaching/cis110/sem2/lectures/ppt/layering.ppt (accessed on 27th September 2013)

TCP/IP model		
Layer number	**Layer name**	**Layer description**
4	Application	Handles high-level protocols (e.g. File transfer protocol), encryption, includes protocols used by most of the applications
3	Transport	Deals with the quality control and error correction of the packet transmission, allows end to end communication
2	Internet	Responsible for the transmission of packets
1	Subnet / Network access	Covers all necessary actions that are needed for IP packet to make a physical link with the receiver

Table 3 – Overview of OSI data layers based on presentation made at Goldsmith Department of Computing[59]

5.4.3. Content layer

This layer contains all the information present in cyber space. This information is everyday accessed, altered and created using email, social networks, websites, blogs and other interfaces accessible in cyber space. Both human and technical users interact with the content layer. As already discussed, the amount of data available in cyber space is immense and it is growing every minute.

5.4.4. Social layer

This layer does not include any technical components, but it covers the people actually using cyber space. Of course that these people interact with the other layers described in this model, but it is the influence of cyber space on people and social groups. This layer covers not only individuals or social groups, but public and private sector as well. It is possible to imagine this layer as the influence of cyber space on the society itself. The influence of cyber space on the societies can be divided into several categories, similar to those discussed above – social, economic, political and military. On the other hand this layer also influences the internet in the most significant way.

5.5. Conclusion

Cyber space has become an important part of everyday lives for millions of people all over the world. The interaction via cyber space became so important that some European countries proclaimed access to the Internet as another basic human right.[60] It

[59] "Layering in Networked Computing", Goldsmiths Department of Computing, University of London, http://doc.gold.ac.uk/~mas01lo/Teaching/cis110/sem2/lectures/ppt/layering.ppt (accessed on 27th September 2013)

[60] BBC, *Finland makes broadband a 'legal right',* (BBC, 2010), http://www.bbc.co.uk/news/10461048 (accessed on 14th November 2013)

is almost impossible, especially for the younger generation, to imagine a world without cyber space. However, the rapid development of cyber space has in some cases overrun the readiness in all four layers of cyber space. Dramatic increase in the amount of data transferred every minute and the increase in the number of users and devices accessing cyber space bring current physical layer to its limits. Any possible disruption of the connection has severe consequences. New types of services in cyber space reveal security issues in the most used protocols in cyber space and the upgrade to more secure environment will be very difficult. The increase in the amount of illegal content is forcing national authorities to increase the activity of police forces in cyber space. In some countries, the so called dangerous content is being filtered or removed from the national cyber space. The increase in the amount of such data is putting national authorities under pressure both from international and national perspective. The rapid development of cyber space and its role in the society has created large differences not only between generations, but also between states. The traditional social patterns have been challenged by cyber space. Not only does mankind face in certain sense challenges brought by the existence of cyber space, the threat of the cyber security issues has to be considered as well.

6. Terrorism

Terrorism is considered to be one of the most serious security risks in Western countries. As a response, governments and responsible institutions implement new security measures in order to minimize the probability of a successful terrorist attack. The implementation is a very complicated process, including necessary legislative changes, new specialized institutions and different approach to security. But the very first step in this process is to identify the risk, which needs to be challenged, namely to define terrorism. Despite the ongoing global war on terror, there is no globally accepted definition of terrorism. Nevertheless, countries across the world have incorporated into their legislative system various definitions of terrorism in order to create the necessary conditions to fight terrorism. Unfortunately, discrepancies in the definitions and different legislative environments under which the definition are applied may lead to different conclusions when answering the fundamental question – what is terrorism?

This chapter describes theoretical background for definition of a term and analysis particular definitions of terrorism. Its aim is to find main aspects of terrorism that have to be addressed in the definition of terrorism to avoid potential misinterpretation and provide information for further analysis, whether the definition of terrorism is applicable to cyber terrorism as well. Analysis of particular definitions will also show which basic features have all definitions in common and what potentially might be the foundation for a globally accepted definition of terrorism.

Evolution of terrorism is another reason why it is important to analyze current definitions. Since the security standards have dramatically changed in previous years, terrorists will likely use different means or strategies, like attacks in cyber space, to achieve their goals. The definition of terrorism is the cornerstone of the security policy. Security policies and particular measures are taken based on the definition of terrorism as stated in the law. If the definition is too narrow, security measures might not be sufficient, thus creating an opportunity for terrorists. The hypothesis for this chapter is that attacks in cyber space would not be regarded as a terrorist act under current definitions of terrorism. If the hypothesis is correct, security measures implemented in order to ensure cyber security might be insufficient or might not take the full advantage of special powers granted by the legislation to fight the terrorism.

For the purpose of this paper definitions of terrorism used in E.U., China, Russia and in the U.S were chosen. These definitions are legally valid in U.N. Security Council permanent member states (given the fact that for United Kingdom and France the E.U. definition is used). More than one American definition of terrorism has been analyzed to demonstrate the complexity and the evolution of the definition of terrorism in the U.S.[61]

6.1. Theoretical background

When analyzing the definitions, two main types of definitions were identified, namely extensional definition and the genus et differentia definition.

Extensional definition formulates its meaning by identifying its extension. This means every object that falls under the definition must be explicitly named or defined. In other words, an extensional definition can be seen as a list of elements, when enlisted elements make the definition. For instance extensional definition of member states of EU would be the list of member countries. In this case, it is feasible to enlist all states to make the definition complete. Such definition can be referred to as an enumerative definition.

Genus and differentia is an Aristotelian pattern of definition. It assigns meaning to a term by putting together two parts. Genus is an already defined term, when differentia further specify genus in such a way that distinguishes it from other subclasses, thus defining a new term. A classical example of genus and differentia definition is the definition of humans as rational animals. There are many ways how to apply this approach on previous example – EU member states. For example, EU member states are all states, which signed the Lisbon Treaty. In this case genus is state because every EU member has to be a state. Differentia part is making the condition state must comply with to qualify as a member state according to this definition – must have signed the Lisbon Treaty.

[61] Given the fact that United States are a major actor in war on terrorism, American definition of terrorism is one of the most important.

Disregarding the theoretical approach used to create a given definition, the definition should clearly define the main characteristics of terrorism. The combination of all this factors must be unique in a way that the definition itself does not leave any space for misinterpretation.

The most important is clearly the definition of terrorism itself, respectively the act of terrorism. Under certain conditions, defining this main aspect might be enough to define clearly terrorism. On the other hand, if the act of terrorism is not unique, e.g. special kind of attack, and it could be executed without necessarily being related to terrorism, other aspects have to be defined. One of them is the actor – who can be considered a terrorist? Again, this aspect has to be defined generally enough to make the definition flexible, but if the definition of the actor, the terrorist, is not distinctive enough, other aspects like motivation, goal or means have to be defined.

For the purpose of this analysis, five main aspects were chosen:

- How is an act of terrorism defined?
- Who can be considered a terrorist?
- What is the goal of terrorism?
- What are the means of terrorism?
- What is the motivation of terrorists?

The analysis itself can be divided into several steps. Firstly, the definition is analyzed from a theoretical point of view – a theory on which is the definition based. Secondly, the analysis of determining part of the definition takes place. Mostly, it is the analysis of differentia part. Thirdly, specific characteristics of each definition are considered. Fourthly, there is a short summary of the definition focused on transferability - the possibility to use the definition globally, flexibility of given definition and complexity. Finally, for each definition is listed the approach towards chosen five aspects.

6.2. Definitions of terrorism

6.2.1. Definition of the U.S. Department of Defense

The current definition by the U.S. Department of Defense as stated in the online dictionary of the Defense Technical Information Centre.

"The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological."[62]

6.2.1.1. Analysis

From a theoretical point of view, this definition is based on the genus and differentia theory, where violence is the genus, which is differentiated afterwards. When attempting to simplify this definition and to find the very substance, it would be calculated unlawful violence generating fear. The rest of the definition focuses on motivation and possibilities. It is interesting to note that this definition counts in the possible threat of violence that could be regarded as terrorism. The unlawful violence has to be calculated. This violence is aimed at governments and societies. It is obvious why governments are mentioned in this definition, especially when considering the motivation of terrorists as stated above. Mainly governments have the power to make such decisions that would fulfill terrorist's demands. A question for further analysis is whether local terrorism can exist and under what conditions.

The motivation of terrorists as stated in this definition is relevant to their goals. The motivation may be political, ideological, or religious. On the other hand, a specific motivation of powerful individuals may exist within a terrorist group. It can be economic profit, personal power, or something else. Generally speaking, the motivation of a terrorist does not necessarily have to correspond to publicly presented goals. For instance, ETA claims that its goal is to create an independent country with its special culture.[63] But what is the real motivation behind? Obviously it can be political independence and freedom. But it can be hunger for power of the organization's leader.

---

[62] Defense Technical Information Centre, *Terrorism,* (Online dictionary of Defense Technical Information Centre, 2011), http://www.dtic.mil/doctrine/dod_dictionary/data/t/7591.html (accessed on 5th May 2011)

[63] Amy Zalman, *ETA,* (about.com, 2011), http://terrorism.about.com/od/groupsleader1/p/ETA.htm (accessed on 11th May 2011)

The relation between presented goals and motivation is rather ambiguous, but the common belief is that there is a direct dependency.

Another interesting aspect of this definition is the threat of violence, which is also considered terrorism. This is a special case, because for other crimes threatening is not judged in the same way as the crime itself. For instance, threatening someone with murder is illegal, but it does not have the same legal consequences as murder itself. This is the way in which this definition highlights the seriousness of terrorism and any activities related to terrorism.

This definition states fear as the first consequence of terrorism. This is very important, because it is fear that actually has the largest impact on the society, not real attacks.

It is possible to derive the total damage caused by planes crashing into the Twin Towers from the $861 million dollars that Industrial Risk Insurers paid to the owners of the buildings in February 2002.[64] The assumed cumulated loss between 2001 and 2009 was calculated to be $38.5 billion,[65] and this is only in the airline industry.

The pressure on governments is defined as a second possible goal of terrorism. The reason why it is so important to mention the external influence on governments lies in Western culture and principles. It is the very basis of democracy that no decision will be taken from the position of force, but on the basis of consensus or majority. That is why it is so important to protect the principles of democracy by defining the use of force as terrorism in order to influence governments.

6.2.1.2. Summary

Despite the fact that this definition of terrorism is very contextual, it is very straightforward. It clearly defines the means of terrorism (use and threat of using violence in order to intimidate governments). Unfortunately, this definition cannot be easily transferred to other legal systems or used on a global basis, because it depends on

[64] Don Paul, J. H. , *The World Trade Center Attack,* (911review, 2011), http://www.911review.com/attack/wtc/index.html (accessed on 5th May 2011)
[65] AirlineFinancials.com, *How legacy airlines lost so much since 9/11,* (AirlineFinancials.com, 2009), http://www.airlinefinancials.com/uploads/09_Aug_How_airlines_lost_so_much_altitude_since_9_11.pdf (accessed on 7th May 2011)

the legal context – this definition of terrorism is based on other definitions. Firstly, the definition of unlawful violence has to be accepted. Subsequently, using the theory of genus et differentia, terrorism can be defined as the use or threat of unlawful violence with a specific goal or motivation. Therefore, it is not possible to use this definition in a different legal system or in a different state if the definition of unlawful violence is not the same. Otherwise the same definition applied in different legal systems would have a completely different meaning. The dependency of this definition has its benefits as well. It is not necessary to modify the definition in order to reflect recent changes in society. It is sufficient to modify the definitions upon which this definition is constructed. It is obvious that this may not be possible in all cases. An example of such modification is, for instance, extending the meaning of violence. Let us assume that under the word 'violence' only violence against human beings is understood. Therefore the definition of terrorism is valid only for violence against humans. If there is a notion that terrorists may attack property in order to achieve their goals, it is necessary to change the definition to cover also violence against property as an act of terrorism (of course under specific conditions). In this case it is not necessary to change the definition of terrorism itself. It might be better and more appropriate to change the definition of violence. This is of course only a theoretical example that disregards the legal process and other legal implications; it only states what is possible due to the form of this definition of terrorism.

Particular aspects are addressed by this definition in following manner:

- How is defined an act of terrorism?

  Calculated unlawful violence or threat of unlawful violence.
- Who can be considered a terrorist?

  Not addressed.
- What is the goal of terrorism?

  Coerce or intimidate governments or societies.
- What are the means of terrorism?

  Inculcating fear.
- What is the motivation of terrorism?

  Political, religious or ideological.

6.2.2. Definition from the National Strategy for Combating Terrorism

The definition of terrorism as used in National Strategy for Combating Terrorism:
"Terrorism—premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents."[66]

6.2.2.1. Analysis

From the point of view of theory, this definition belongs to the group of genus and differentia definitions. Violence is the genus, while the differentia can be divided into several groups. The first is the character of violence – premeditated and politically motivated; the second is the object of violence – noncombatant targets; and the third is the causative agent – subnational groups or clandestine agents.

In this definition of terrorism, politics is considered to be the only motivation for terrorists. The first possible thought that might occur is that this is not correct, as the media often report on terrorist groups proclaiming religious war against infidels. On the other hand, it is possible to say that ideological or religious motivation also has its political implications. Therefore, it is sufficient to state a political motivation in the definition of terrorism. Several questions arise from this assumption. Would it be just a crime if there were an attack on people of another religion, presented as necessary and holy in order to praise only the right god? Using this definition, it would be very difficult to prove that there is political motivation involved so that it could be regarded as an act of terrorism.

This brings us to the target of the violence – noncombatant targets. The Geneva Conventions distinguish between civilians and noncombatant personnel. Generally speaking, the term 'civilian' does not include soldiers, even if they cannot participate in military operations. Despite the unanswered question why it is so important to state 'noncombatant' instead of 'civilian' in this definition, there is no doubt that this definition takes into consideration only living targets. It omits the critical infrastructure, key institutions and other material targets.

---

[66] U.S.Government, *National Strategy for Combating Terroris,* (U.S.Government, 2003) http://www.upmc-biosecurity.org/website/resources/govt_docs/public_health_prep/whitehouse/whitehouse_national_strategy_for_combating_terrorism.html (accessed 11th May 2011)

The causative agent in this case is a subnational group or clandestine agent. 'Subnational group' is a very appropriate term provided that terrorism cannot be perpetrated by states. If so, it would not be terrorism, but war or other violation of international law and the Geneva Convention. Nevertheless, mentioning clandestine agents as possible perpetrators does not exclude the role of states or governments completely.

6.2.2.2. Summary

This definition is again very short. As in the previous definition, it depends on other definitions. This prevents its transferability or global acceptance. Given its form it seems that the definition was formed only to be used in this particular document. It completely omits potential targets of terrorism. This definition is not so clear in comparison with the definition by the U.S. Department of Defense. The main reason lies in the use of the term 'noncombatant target'. This contextual aspect limits the use of the definition. This supports the hypothesis that the definition was intended only for the National Strategy for Combating Terrorism. The readers of this document were probably familiar with the term 'noncombatant' and, therefore, such definition was very clear to them. The definition may be considered too vague in certain aspects, but in others it is very specific – especially when defining possible terrorists.

Particular aspects are addressed by this definition in following manner:

- How is defined an act of terrorism?

  Premeditated violence.
- Who can be considered a terrorist?

  Subnational groups or clandestine agents.
- What is the goal of terrorism?

  Not addressed.
- What are the means of terrorism?

  Not addressed.
- What is the motivation of terrorism?

  Political.

6.2.3. Definition from the Code of Federal Regulations

Definition used in the Code of Federal Regulations revised on 1st July 2010.

"Terrorism is the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."[67]

6.2.3.1. Analysis

From a theoretical point of view, this definition belongs to genus and differentia type, despite the fact that in this case the differentia part is very extensive. Attempting to simplify the definition, terrorism can be defined as unlawful violence with political or social objectives. The rest of the definition specifies the possible targets of the unlawful violence.

In comparison with other definitions, threatening is not mentioned in this definition. On the other hand, it says 'unlawful use of force and violence'. The question is whether unlawful use of force can be different from violence, and therefore needs to be specifically mentioned in the definition. Moreover, to define potential subjects affected by terrorism, the definition mentions persons, without specifying the nature of these persons (civilians, noncombatants, etc.). It also mentions property as a potential target. This is very interesting because moving on to potential decision makers influenced by terrorism, the definition mentions governments in the first place. Without distinguishing between private and public property, this definition suggests that terrorists can damage private property in order to influence governments. Again, the role of governments in this definition is clear – they have the power to fulfill terrorists' demands. But why is civilian population stated as potential subject of intimidation? The example of Spain illustrates that mentioning population or its segment in the definition of terrorism is appropriate. The Spanish government maintained the direction of its foreign policy after the terrorist attacks in Madrid in 2004, but it was the population who voted for the party promising to withdraw troops from Afghanistan, thereby fulfilling the demands of terrorists. Such intimidation, resulting in a democratic change in foreign policy, can only be applied in democratic countries, because the population does not have other possibilities than elections to influence the foreign policy of the country. In any other

[67] U.S.Govrnement, *Code of Federal Regulations*, (U.S.Government, 2010), Title 28, Chapter I, Section 0.85, http://www.law.cornell.edu/cfr/text/28/0.85 (accessed on 13th May 2011)

political system the population can only influence the decision makers indirectly and with limited results. The possibility of a revolution or other movement is very limited, because it brings uncertainty and destabilization. These possible risks of other then political pressures on the government equal or even outweigh the risk of another terrorist attack.

In the end, the definition states possible motivations for the terrorists – political or social objectives. Political objectives are again very clear – a change in foreign policy for instance. It is more difficult to understand why it is necessary to point out social objectives, and what kind of terrorists would pledge to have social objectives. It can possibly refer to uprisings of lower-income groups discontented with the social situation. It is a question for further analysis whether it is necessary to use the term 'terrorist' in this case, but that is not the goal of this dissertation.

This definition specially mentions property as a potential target of terrorist attacks, and concedes the possibility that destroying or damaging property can influence governments. Another interesting aspect is that the civilian population or any segment thereof, as a possible target of terrorist activities, is treated in a different way. Terrorists usually attack or threaten to attack civilians in order to create pressure on governments. But in this definition, the population or its segments are put on the same level with governments. This leads us to the conclusion that according to this definition, the population or its segment is able to fulfill terrorists' demands. Again, it is necessary to mention that this is only true under certain conditions, for example only in democratic countries, where the population can influence national policies through elections.

6.2.3.2. Summary

This definition of terrorism is very clear and answers most of the questions that need to be answered. It states the goal of terrorism (accomplishing political or social objectives), the act of terrorism (unlawful violence) and the means of terrorism (intimidating government). However, the definition does not include threat as an act of terrorism. Despite the fact that some of its elements are questionable, this definition is understandable and it is easy to modify it by changing its differentia part. Again, it would be very difficult to use this definition in other countries.

Particular aspects are addressed by this definition in following manner:

- How is defined an act of terrorism?
  Unlawful use of force and violence.
- Who can be considered a terrorist?
  Not addressed.
- What is the goal of terrorism?
  Intimidate or coerce a government, the civilian population, or any segment thereof.
- What are the means of terrorism?
  Not addressed.
- What is the motivation of terrorism?
  Political or social.

6.2.4. Definition of the FBI

The current definition of FBI as used in the publication Terrorism 2002 – 2005 is:
"Domestic terrorism is the unlawful use, or threatened use, of force or violence by a group or individual based and operating entirely within the United States or Puerto Rico without foreign direction committed against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives.

International terrorism involves violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state. These acts appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by assassination or kidnapping. International terrorist acts occur outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum."[68]

[68] FBI, *Terrorrism 2002/2005,* (FBI, 2006), page 5, http://www.fbi.gov/stats-services/publications/terrorism-2002-2005/terror02_05.pdf (accessed on 17th May 2011)

6.2.4.1. Analysis

In this FBI publication there are two definition of terrorism – domestic and international. A common expectation would be for the definition of international terrorism to be the same as that of domestic terrorism, only containing an international element like the origin of terrorists, etc. But the definition of international terrorism is more specific. The definition of domestic terrorism does not explicitly mention assassination or kidnapping. Another important difference is that property is not explicitly mentioned in the definition of international terrorism. Other parts of the definition do not include property as a potential target of terrorist attacks. The definition explicitly mentions kidnapping, assassination and violent acts dangerous to human life, which are all violations of criminal laws. In the end of the main definition is the definition of the international element.

For further analysis only the definition of international terrorism will be taken into consideration, because in our globalised world terrorism without an international element is not very probable.

From a theoretical point of view, this definition of terrorism is based on the genus and differentia theory, but aspects of extensional definition are also present in the term. In this case, a violent act is the genus. The differentia is slightly more complicated – it contains the possible goals of terrorism (intimidating civilian population, influencing government), while pointing out specific actions that would be regarded as terrorist acts. This is the part based on extensional definition. Pointing out assassination and kidnapping is not necessary for the definition itself. Assassination is definitely dangerous to human life and represents a violation of criminal laws as well. It can always have a political motive; therefore, assassination can be used to influence governments or intimidate the civilian population. The reason for specifically including assassination and kidnapping in the definition may be practical rather than legal. It gives the impression that such activities are taken into consideration and would not be considered surprising. Also a possible terrorist can assume that security measures and strategies based on this definition count with the possibility of assassination or kidnapping.

It is interesting to note that this definition does not explicitly mention the threat of violence. This is even more surprising given the fact that the definition states assassination and kidnapping as possible terrorist acts. It is true that kidnapping usually leads to blackmailing, but still it is logical to expect terrorist to threaten their possible target first. This is more obvious in the case of assassination. Terrorists can threaten to assassinate someone in case that their demands are not met, but their position would not be so strong if they first assassinated someone and afterwards presented their demands.

The international element in this definition is also interesting. It is understandable that the definition covers international aspects in terms of international cooperation, seeking asylum abroad, etc. But the definition does not say it covers only terrorist acts with an international element carried out in the U.S. The definition also says that terrorism is a violent act dangerous to human life that would be a criminal violation if committed within the jurisdiction of the United States. This part of the definition suggests that the US jurisdiction is superior to others. Probably these legal discrepancies are not important, because they are limited by the competency of FBI or by other federal regulations; it is, however, a very interesting point.

6.2.4.2. Summary

This definition combines two theoretical approaches – extensional definition and genus and differentia definition. The length of the definition and the combination of two different theories make it more difficult to understand as well as to apply. Both the domestic and international terrorism definitions have the advantage of being very adjustable, particularly by modifying the extensional part of the definition. On the other hand the discrepancies between domestic and international terrorism diminish the credit of these definitions. Nevertheless, the extensional part of the definition is transferable. Kidnapping and assassination as possible terrorist acts can be easily transferred to a different legal system or accepted on a global level.

Particular aspects are addressed by this definition in following manner:

- How is defined an act of terrorism?
  Violent acts or acts dangerous to human life.
- Who can be considered a terrorist?
  Not addressed.
- What is the goal of terrorism?
  Intimidate or coerce a civilian population, influence the policy of a government, or affect the conduct of a government.
- What are the means of terrorism?
  Intimidation, coercion, assassination or kidnapping.
- What is the motivation of terrorism?
  Not addressed.

6.2.5. Definition of the Council of the European Union

The initial document for EU definition of terrorism is the Council Common Position presented on 27th December 2001, which defines a terrorist act as follows:

„… 'terrorist act'

shall mean one of the following intentional acts, which, given its nature or its context, may seriously damage a country or an international organization, as defined as an offence under national law, where committed with the aim of:

(i) seriously intimidating a population, or

(ii) unduly compelling a Government or an international organization to perform or abstain from performing any act, or

(iii) seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization:

(a) attacks upon a person's life which may cause death;

(b) attacks upon the physical integrity of a person;

(c) kidnapping or hostage taking;

(d) causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed plat- form located on the continental shelf, a public place or private property, likely to endanger human life or result in major economic loss;

(e) seizure of aircraft, ships or other means of public or goods transport;

(f) manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons;
(g) release of dangerous substances, or causing fires, explosions or floods the effect of which is to endanger human life;
(h) interfering with or disrupting the supply of water, power or any other fundamental natural resource, the effect of which is to endanger human life;
(i) threatening to commit any of the acts listed under (a) to (h);
(j) directing a terrorist group;
(k) participating in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the group."[69]

6.2.5.1. Analysis

From a theoretical point of view, this definition consists of two different approaches. The first approach is used for the beginning of the definition and belongs to the genus and differentia type. The rest of the definition, stating every possible aim and means of terrorism, represents the extensional approach to defining terrorism.

The genus and differentia part, in its very essence, defines a terrorist act as an illegal act (intentional act, …, defined as an offence under national law) that may damage a country or an organization. The genus is represented by the act, 'illegal' and 'damaging country or organization' is the differentia. It is interesting to note that this definition does not specify the terrorists' possible motivation, unless the motivation is included in the context of the act. Neither does this definition clearly state the nature of a terrorist act in this part; it merely says, "May seriously damage a country or an international organization." The nature of the terrorist act itself is also very peculiar – "given its nature or its context", especially when considering that this is the most important part of the definition. The nature or context of the act is the distinguishing feature between an act of terrorism and an offence against the law. A possible act of terrorism does not

[69] E.U. Council, *Council Common Position (2001/931/CFSP),* (E.U. Council, 2001), http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32001E0931&model=guichett (accessed on 5th May 2011)

necessarily have to be a violent act; it is sufficient if the context of the act corresponds to this definition. Again, this part is further specified in the extensional part.

The extensional part of the definition is very detailed; it states an extensive range of activities that, under specific conditions, may be regarded not only as crimes, but also as terrorist acts. Despite the intention to make it very precise by listing the acts explicitly, the definition is unclear in certain points. For instance in bullet (iii) the definition mentions structures as possible targets of terrorist acts. It defines the nature of the structures, but the term is still rather vague when compared to the very specific definition of possible attacks in bullet (b). The fact that the extensive list also includes threatening as a possible act of terrorism is very important. Such threats, however, can only be considered as terrorist acts if they have certain other features, as stated in the first part of this definition. This can be demonstrated on the example of a phone call reporting a bomb in a school. Obviously, it is a violation of national law, but it is unlikely to be considered as an act of terrorism. The level of detail in this extensional part of definition is sometimes stunning. For example, under bullet (d) is a fixed platform located on the continental shelf. This level of detail might seem irrelevant, but it has its place in this definition, especially in the context of continental law.

6.2.5.2. Summary

This definition of terrorism combines two theoretical approaches, with accent placed on the extensional definition theory. The extensional part, despite its explanatory value, is too long and makes this definition very complex. The definition goes into great detail in certain aspects, but in other cases it uses only very vague terms. It is easy to modify this definition by simply adding another bullet to the list. If the extensional part does not use other definitions or contextual terms, it can be used on a global level. The extensional definition may be easier to apply, because it is very clear and provides a high level of detail. On the other hand, the public may find it difficult to accept such a complex definition. Given the legal context and traditions of the European Union, this definition is coherent with the majority of European legal systems – it is extensional, very comprehensive, and it covers all aspects without the need to study other materials and definitions. In this respect it resembles any other legal act.

Particular aspects are addressed by this definition in following manner:

- How is defined an act of terrorism?
  Intentional act specified under bullet points (a) to (h) including threatening to commit any of the listed acts.
- Who can be considered a terrorist?
  Not addressed.
- What is the goal of terrorism?
  Not addressed.
- What are the means of terrorism?
  Addressed under bullet points (i), (ii), and (iii).
- What is the motivation of terrorism?
  Not addressed.

6.2.6. Russian Definition of Terrorism

The most important definition of terrorism used in Russia was created as a reaction to attacks executed by Chechen rebels in 1995, 1996. Terrorism is defined by federal law no.130 – FZ. It was signed by Russian president Boris Yeltsin in 1998. It defines terrorism as follows:

"Terrorism is violence or the threat of violence against individuals or organizations, and also the destruction (damaging) of or threat to destroy (damage) property and other material objects, such as threaten to cause loss of life, significant damage to property, or other socially dangerous consequences and are implemented with a view to violating public security, intimidating the population, or influencing the adoption of decisions advantageous to terrorists by organs of power, or satisfying their unlawful material and (or) other interests; attempts on the lives of statesmen or public figures perpetrated with a view to ending their state or other political activity or out of revenge for such activity; attacks on representatives of foreign states or staffers of international organizations enjoying international protection, and also on the official premises or vehicles of persons enjoying international protection if these actions are committed with a view to provoking war or complicating international relations."[70]

[70] Committee of Experts on Terrorism, *Federal law no.130 – FZ.,* (Russian Governement, 1998) http://fas.org/irp/world/russia/docs/law_980725.htm (accessed on 5th May 2011)

6.2.6.1. Analysis

Terrorism would be defined in a simplified way as violence or a threat of violence against individuals or organization with a view to violate public security, intimidate the population or influence the government. In this simplified version it is easy to see the influence of genus et differentia theory. Violence or threat of violence is the genus and other parts specifying the nature of violence to clearly define terrorism. In this case, the differentia part focuses on targets and on the motivation of perpetrators. According to this simplified definition, any violence against individuals violating public security can be seen as an act of terrorism.

Nevertheless, the definition is much more complex. The complexity is the result of using the extensive approach to the definition. It is visible in the first part that not only violence or threat of violence is the subject of the definition, it is also the destruction, threat to destroy, attempts on the lives of statesmen, attacks on the representatives of foreign states, etc. All these particularly named actions can be seen as acts of terrorism under specific conditions. The second part of the definition further elaborates on special cases and particular characteristics that can make an attack to be defined as an act of terrorism. This can be seen at the end of the definition: "(attacks)...on the official premises or vehicles of persons enjoying international protection if these actions are committed with a view to provoking war or complicating international relations."

The definition resembles others analyzed in this paper. However, several formulations are very interesting, for instance the usage of the term public security. It is a rather vague term to be used in such definition, because it is easy to declare that certain activity presents a threat to public security. It might be sufficient to declare that violence can be defined as terrorism when it is executed with the aim to intimidate population or influence the government, making the use of term public security redundant.

Another interesting aspect is the attack on the life of statesmen as mentioned in this definition. According to this definition, any attack on public figure or statesmen is an act of terrorism. It is speculative how much this aspect of the definition is influenced by the political culture in Russia, but this is not in the planned scope of this paper. Particularly listed example of terrorism is the attack on representatives of foreign states. First part of

the definition defines that any violent attack on individual with certain aspirations can be seen as terrorism. Again, this case might be already addressed by the first part, but for unknown reasons it is explicitly mentioned in this definition.

6.2.6.2. Summary

The Russian definition of terrorism is based on both theoretical approaches, while majority of potential terrorist attacks is addressed by the genus et differentia part. The extensive part of this definition highlights special acts, which would also be considered as acts of terrorism. The combination of two theoretical approaches creates a complex definition difficult to assess. Only the extensive parts of this definition can be used globally, as the genus et differentia part is based on local legal system and cannot be easily transferred.

Particular aspects are addressed by this definition in following manner:

- How is defined an act of terrorism?
  Violence or the threat of violence, destruction (damaging) of or threat to destroy (damage) property and other material objects, attempts on the lives of statesmen or public figures, attacks on representatives of foreign states or staffers of international organizations.
- Who can be considered a terrorist?
  Not addressed.
- What is the goal of terrorism?
  Influencing the adoption of decisions advantageous to terrorists by organs of power, or satisfying their unlawful material and (or) other interests. In case of statesmen it is ending their state or other political activity or out of revenge for such activity. In case of foreign representatives it is provoking war or complicating international relations.
- What are the means of terrorism?
  Violating public security, intimidating the population, or influencing the adoption of decisions
- What is the motivation of terrorism?
  Not addressed.

6.2.7. Chinese definition of terrorism

Decision of the Standing Committee of the National People's Congress on Issues concerning Strengthening Anti-Terrorism Work
(Adopted at the 23rd meeting of the Standing Committee of the 11th National People's Congress on October 29, 2011):

"Terrorist activities are activities conducted by violence, destruction, intimidation and other means to create social panic, endanger public security or threaten state organs or international organizations and causing or attempting to cause casualties, grave property loss, damage to public facilities, disruption of social order and other severe social harm, as well as activities to assist the above activities by instigation, financing or any other means.
Terrorist organizations are criminal groups formed for conducting terrorist activities.
Terrorists are individuals who organize, plan or conduct terrorist activities and the members of terrorist organizations."[71]

6.2.7.1. Analysis

The Chinese definition does not define terrorism itself, but it consists of three separate definitions. The first definition describes terrorist activities while the second and the third definition cover potential perpetrators – terrorists and terrorist groups.

The definition of terrorist activities is based on the extensive approach. It is simply a list of activities that can be considered as terrorism. Apart from main terrorist activities like using violence or destroying property, this definition covers also supportive activities like providing financial support.

Unfortunately, the Chinese definition of terrorist activities is not very good from the theoretical point of view. First of all the differentiation of activities is not very sound. Practically, any activity might be considered as a terrorist activity, when it may endanger public security or cause other severe social harm. The definition does not state that such an activity must be illegal, so theoretically demonstration might be considered

[71] National People's Congress, *Decision of the Standing Committee of the National People's Congress on Issues concerning Strengthening Anti-Terrorism Work,* (NPC, 2011), http://en.pkulaw.cn/display.aspx?id=9082&lib=law (accessed 11th May 2012)

as a terrorist activity, because it may lead to social harm. Neither does the definition address in any way possible motivation of terrorist groups. Secondly, the differentiation of terrorist activities is also rather vague and it does not clearly define the border between criminal and terrorist act. For example homicide without political motivation would hardly be considered as a terrorist act. Nevertheless, Chinese definition declares that any violent activity causing casualties is a terrorist activity. Even "simple" homicide complies with this definition. The same logic can be applied on sprayers, as the graffiti is without doubt damage to public facility.

The following definitions of a terrorist and a terrorist organization are based on the definition of terrorist activity. Interesting is the definition of terrorist organization, when the basis of the definition uses the term "criminal group." Logical conclusion would lead to the statement that only criminal groups can execute terrorist activities. But as discussed before, terrorist activities do not have to be necessarily criminal acts. Probably other logic is applied in this case – forming a group to execute terrorist activities is considered as a criminal act, therefore terrorist group is in the same time a criminal group. This only highlights internal inconsistency in the definition of terrorism in China.

6.2.7.2. Summary

Despite the fact that this definition seems to be very complex when defining terrorist activities, it does not give enough supporting features that would enable to distinguish between mere criminal and terrorist activities. Since this definition is incorporated in the law, the responsibility of taking final decision when defining terrorist activities is in the hands of judges. They have to decide whether the nature of given act brought to trial comply with the definition of terrorist activities or not. Unfortunately, it is theoretically possible to apply this definition to common criminal acts, which would not be regarded as acts of terrorism using other definitions analyzed in this paper, as discussed in the analysis. This definition describes the terrorist activities, but to fully comply with the theory of genus et differentia, it would by necessary to define other features like motivation or goals of such activities in differentia part. Therefore this definition could be used only as a foundation for global definition, mainly the extensive list of activities being regarded as terrorism.

Particular aspects are addressed by this definition in following manner:

- How is defined an act of terrorism?
  Activities conducted by violence, destruction, intimidation and other means.
- Who can be considered a terrorist?
  Individuals.
- What is the goal of terrorism?
  Not addressed.
- What are the means of terrorism?
  Create social panic, endanger public security or threaten state organs or international organizations and causing or attempting to cause casualties, grave property loss, damage to public facilities, disruption of social order and other severe social harm
- What is the motivation of terrorism?
  Not addressed.

6.3. Results

Following chart shows which aspects were addressed by each definition.

Aspect / Definition	U.S. Department of Defense	National Strategy for Combating Terrorism	Code of Federal Regulations	FBI	Council of the E.U.	Russian	Chinese
How is defined an act of terrorism?	Calculated unlawful violence / threat	Premeditated violence	Unlawful use of force / violence	Violent / dangerous acts	*Extensive list*	Violence, destruction / threat	Violence, destruction or intimidation
Who can be considered a terrorist?	N/A	Subnational groups / clandestine agents	N/A	N/A	N/A	N/A	Individuals
What is the goal of terrorism?	Coerce or intimidate governments / society	N/A	Intimidate or coerce government /population	Intimidate or coerce population / government	Intimidate or compel population / government, destabilize	Influence government, provoke war or complicate international relations	N/A
What are the means of terrorism?	Inculcate fear	N/A	N/A	Intimidation, coercion, assassination or kidnapping	*Extensive list*	Violation of public security, intimidation of population	Social panic, endanger public security, …
What is the motivation of terrorism?	Political, religious or ideological	Political	Political or social	N/A	N/A	N/A	N/A

6.3.1. How is defined an act of terrorism?

Most of the definitions analyzed on previous pages contain 'unlawful violence' or 'use of force' as the definition of a terrorist act. Of course, the definition may contain an explicit list of activities that may be considered as terrorist acts, such as the definition adopted by the EU Council, but for the definition of the genus and differentia type unlawful violence is a very clear beginning. On the other hand, it is necessary to be more specific to fully answer this question. Not only unlawful violence itself, but also the threat of unlawful violence can be considered an act of terrorism if other conditions are met. Terrorist threats are very dangerous for the stability of a country, which is why also threatening has to be included in the definition of terrorism.

6.3.2. Who can be considered a terrorist?

The previous answer states that a terrorist act is basically an act of unlawful violence – violence breaking national law. This means that direct terrorism[72] cannot be perpetrated by states or by supranational bodies. States cannot perpetrate[73] terrorism because they are not bound by national law of other states, but by international law. If a state was performing actions similar to acts of terrorism, it would be regarded as breaking international law, the Geneva Conventions and other international agreements. In other words, states can make war, but not commit direct acts of terrorism.

On the other hand, it is necessary to admit the possibility of states supporting or tolerating terrorist organization or members of terrorist groups. Nevertheless, sovereign states are bound by international law and possible sanctions should be based on international law.

Using the opposite approach, the question whether a single individual can be a terrorist emerges. Despite the fact that recent terrorist attacks are usually executed by members or followers of terrorist groups, a single individual can be identified as a terrorist, like in the following case.

---

[72] Direct form of terrorism – meaning active and public participation in terrorist activities.
[73] Supporting terrorism or particular terrorist organization is a different situation.

"On July 4, 2002, Hesham Mohamed Ali Hedayat began shooting randomly while standing in line at the ticket counter of El Al Israeli National Airlines at the Los Angeles International Airport. During the attack, an El Al ticketing agent and a bystander were killed. Hedayat was subsequently killed by an El Al security officer. A worldwide investigation determined that Hadayat's religious and political beliefs were the primary motivation for the attack, and not personal revenge. Following these investigative findings, this case was officially designated as an act of international terrorism".[74]

Despite the possibility of an individual being a terrorist, for the purpose of defining terrorism the term 'sub national group' is acceptable as an answer to the question.

6.3.3. What is the goal of terrorism?

Terrorists' goals can be divided into two categories: enforcing change and resisting change. It is obvious that such a narrow division of terrorists' goals is very vague, but looking more close, it might be appropriate. Let's take the attitude of Hamas towards Israel as a model of resisting change. Hamas has never officially acknowledged the creation of the state of Israel, and its actions are aimed against Israel. Bomb attacks in Spain, resulting in a change of government, are an example of enforcing change. In this case the aim was to change current foreign policy and to withdraw troops from Afghanistan.

Accepting the view that a terrorist group is an extremely radical political party, it is possible to say that terrorists enforce or resist changes they cannot bring about by using standard political procedures used in a particular country. If the country is a democratic one, terrorists are usually a minority and are not able to enforce their goals through elections.

Analyzed definitions state different examples of terrorists' goals, but in general it is to force government to take certain action.

---

[74] FBI, *Terrorrism 2002/2005,* (FBI, 2006), page 10, http://www.fbi.gov/stats-services/publications/terrorism-2002-2005/terror02_05.pdf (accessed on 17th May 2011)

6.3.4. What are the means of terrorism?

The main means of terrorism is fear. Fear among the population disrupts standard behavior patterns, resulting in stress end economic loss. Of course the amount of fear evolves in time, and also corresponds to the security measures adopted. To install fear, terrorists do not really need to carry out a terrorist attack; it is enough for them to pronounce the possibility of doing so and extensively present this idea in global media. Of course it is necessary to support such proclamations by demonstrations of force – by carrying out real attacks. Sometimes an attack is not only the means, but also the goal. If the target is a key decision maker, potential success may support the opinion about the terrorists' capability, as well as help to enforce or resist a change. For instance, the assassination of Yitzhak Rabin not only proved that the right wing extremists are capable terrorists, but also seriously halted the peace process.

Another important fact is that fear causes significantly more economic damage than a terrorist attack itself, as already discussed.

6.3.5. What is the motivation of terrorism?

Motivation of terrorists depends on their goals. The presented goal of Hamas is to destroy Israel,[75] therefore the motivation is presumably political. Terrorist attack in Japan in the 90's executed by Aum Shinrikyo were supposed to prepare the world for the religious change, therefore the motivation was religious.[76]

Nevertheless, it is necessary to distinguish between presented motivation of terrorist groups and the possible motivation of individual members, especially leaders of terrorist groups. Again, it is possible to apply the same principles as on the political parties – leader of political party does not have to believe in the publicly presented political goals and motivation, but following his personal goals and motivation he accepts his role in the party

[75] Israel Foreign Ministry, *The Covenant of the Hamas,* (Israel Foreign Ministry, 1988), http://www.fas.org/irp/world/para/docs/880818a.htm (accessed 2nd February 2012)
[76] Tom Mangold, Jeff Goldber, *A mnoho lidí zemřelo...pravda o biologických válkách,* (Themis: Praha, 2001), pages 359 - 375

to achieve them (e.g. to become rich and powerful proclaiming social solidarity and savings).

Another factor regarding possible motivation of terrorists is the size and ability of the terrorist group. Originally, the goal of Taliban was to fight Russian army in Afghanistan. The motivation was therefore political and territorially limited. But nowadays the goals of Taliban are more global and so is the motivation. But it is necessary to admit that the motivation, goals and territory do not have to be in equal proportion. Even small terrorist group with local influence might have global goals and motivation.

However, the motivation described in most of the definitions is political, religious and ideological. Some definitions mention also social motivation in terms of their goals – to create social instability etc. The motivation of terrorist can be various. Therefore the contribution of this aspect to the definition of terrorism is very limited.

6.4. Global definition of terrorism

Many differences between analyzed definitions of terrorism were presented. Definitions are based on different theoretical approach, they address particular aspects of terrorism in a particular way and they stress different factors. It is possible to say that in some cases the object of the definition is different. As the American definitions, despite being different, stress the unlawful violence on civilian population, possibly as the result of 9/11 attacks. The terrorism from American prospective is violent attack aimed at civilians. On the other hand, Chinese and Russian definitions are more focused on social stability and order since the terrorism is regarded rather as an activity aimed at disrupting current state and destabilizing the society. There is undoubtedly a dependency between the main focus of the definition and the most severe danger terrorism presents from the governmental point of view.

There are many obstacles in the way to adopt common definition of terrorism to support ongoing war on terror. Firstly, every nation has different perception of terrorism related to its particular experience and legal system. Secondly, based on the theoretical approach of

the definition, the meaning might be different under given legal conditions. This applies mainly for genus et differentia definition. And thirdly, every state wants to address by the definition of terrorism particular form of terrorism, which is regarded as the most dangerous.

Therefore it is highly improbable that global and thorough definition of terrorism would be accepted soon. However, it is possible to find a consensus between states on the definition of terrorism. Such example is the definition of the E.U. Commission. Despite the fact that this definition is very detailed, technical and mainly based on extensional approach, it is a precedent proving that it is possible to find a compromise. The extensional approach to define terrorism brings the opportunity not to reach an agreement on the definition of the terrorism completely, but to define particular terrorist acts or types of attacks that will be regarded as terrorist acts. Accepting this approach will not lead to a thorough definition of terrorism in a short term, but it will make possible to agree on basic terrorist acts.

6.5. Terrorist or freedom fighter

The definitions of terrorism were discussed so a terrorist can be defined as well. However, during Arabian Spring in 2012 that part of the world was calling the fighters against established regimes rebels, opposition or freedom fighters, while other countries were calling them terrorists. How it is possible to see completely opposite opinions? Let's simply describe the actions that took place in Tunisia, Egypt or Libya.

At first, it was usually a peaceful demonstration. Nevertheless, the aim of such demonstrations was to intimidate the government to undertake certain actions, like resignation or significant changes of current legal system. Such actions would not be described as violent acts. However, according to definitions of terrorism valid in Russia or in China such action could have been regarded as an act of terrorism. Secondly, those peaceful demonstrations turned into violence. It is impossible to decide whether the wave of violence was caused by pro-governmental provocateurs or simply by the frustration of the people. So far all definitions that have been analyzed would consider such action as a

terrorist activity. How come that the United States did not interfere to support the government against terrorists as a part of global war on terror?

One of the first thoughts about the right to revolt is from John Locke. In his book Two Treatises on Government he declares:
"... whenever the Legislators endeavor to take away, and destroy the Property of the People, or to reduce them to Slavery under Arbitrary Power, they put themselves into a state of War with the People, who are thereupon absolved from any farther Obedience, and are left to the common refuge which God hath provided for all men against force and violence. ... [Power then] devolves to the People, who have a Right to resume their original Liberty, and, by the Establishment of a new Legislative (such as they shall think fit) provide for their own Safety and Security, which is the end for which they are in Society."[77]

Locke's ideas were one of the major influences helping to formulate American Constitution. This influence is visible, for instance, in the Declaration of Liberty, when the reasons for the separation from Great Britain are given:

"…But when a long train of abuses and usurpations, pursuing invariably the same Object evinces a design to reduce them under absolute Despotism, it is their right, it is their duty, to throw off such Government, and to provide new Guards for their future security."[78]

Despite the fact that in the Constitution itself the right to revolt is not granted, it is possible to find several formulations of this law in particular bills of rights. For instance, the Bill of Rights of New Hampshire declares in article 10:

"[Right of Revolution.] Government being instituted for the common benefit, protection, and security, of the whole community, and not for the private interest or emolument of any one man, family, or class of men; therefore, whenever the ends of government are perverted,

[77] John Locke, *Second Treatise of Civil Government,* (Cambridge University Press: Cambridge, 1960), chapter 3, paragraph 222
[78] Continental Congress, *The Declaration of Independence*, (ushistory.org, 1995), http://www.ushistory.org/declaration/document/ (accessed on 16th May 2011)

and public liberty manifestly endangered, and all other means of redress are ineffectual, the people may, and of right ought to reform the old, or establish a new government. The doctrine of nonresistance against arbitrary power, and oppression, is absurd, slavish, and destructive of the good and happiness of mankind."[79]

Similar articles stating that the supreme power is in the hands of people can be seen in: Kentucky Bill of Rights, Pensylvanian Declaration of Rights, Tennessee Constitution, Declaration of Rights of North Caroline and in others.

That only highlights the fact that American constitution and legal system was based on the experience of a nation that fought for its freedom against their king and government. The British people would probably describe American freedom fighters as terrorists, if the world terrorist had existed in that time. But this historical experience is not shared by all countries and therefore different opinions on such matters exist among some states. It is necessary not to forget political circumstances, which may modify otherwise clear opinion to suit political interests. Nevertheless, the simplified conclusion might be that in case of civil uprising or revolution, those who win are usually freedom fighters while those who lose are considered as terrorists.

6.6. Definition of cyber terrorism

First of all it is necessary to decide, whether a definition of terrorism is applicable to cyber space. If not, it means cyber space is so different that it needs a definition of terrorism on its own – definition of cyber terrorism. In this case it would be necessary to acknowledge cyber space as independent from the real world. This would lead to creating an independent definition of cyber terrorism having a limited relationship to the definition used outside of cyber space. In such a case it would also be possible that the definition would include different activities such as, for instance, publishing classified information. The obvious disadvantage of this concept is the possible inconsistency between the definition of cyber terrorism and terrorism. This could lead to an awkward situation where a particular action

[79] Congress of New Hampshire, *Bill of Rights,* (nh.gov, 2007), article 10, http://www.nh.gov/constitution/billofrights.html (accessed 21st June 2011)

committed in cyber space would be considered as an act of terrorism, while it would be classified as a crime in the real world, and vice versa. Provided that definition of terrorism is universal and therefore valid for cyber space as other laws, it is necessary to analyze if cyber attacks would comply with the definition of terrorism.

The analysis of used definitions of terrorism focused on following aspects:

- How is defined an act of terrorism?
- Who can be considered a terrorist?
- What is the goal of terrorism?
- What are the means of terrorism?
- What is the motivation of terrorism?

Cyber attacks can comply with the definitions in terms of goal, means and motivation. For instance, a particular server can be targeted and damaged by the perpetrator in order to spread fear among the population, supporting his final goal of persuading the government to do certain action according to his political motivation. This would be perfectly coherent with all analyzed definitions in terms of goals, means and motivation. Those three factors in general also make the difference between cyber terrorism and cybercrime, as discussed above.

Only some definitions define who can be a terrorist. But a terrorist can commit a bomb attack as well as denial of service (DoS) attack, so cyber attacks would comply with all definitions on this condition.

The most important aspect is how the definitions define an act of terrorism. Many definitions operate with the term violence, as discussed above. Therefore a cyber attack would be regarded as an act of terrorism only if the cyber attack could be regarded as violence. Intruder might cause physical damage using internet in some cases, for instance causing explosion of gas pipes or changing traffic lights, but can the activity itself, like installing computer virus or changing line of code, be regarded as violence? Breaking cyber security, installing malicious software, corrupting data, all these activities are realized in

cyber space and have nothing in common with physical force, whereas the common understanding of violence is based on the physical force. Oxford dictionary defines violence as follow: "Behaviour involving physical force intended to hurt, damage, or kill someone or something."[80]

Very similar description is used in the legal definition of crime of violence:

"The term 'crime of violence' means—
(a) an offense that has as an element the use, attempted use, or threatened use of physical force against the person or property of another, or
(b) any other offense that is a felony and that, by its nature, involves a substantial risk that physical force against the person or property of another may be used in the course of committing the offense."[81]

From the legal perspective violence is always connected to the use of physical force, which is not present in cyber space. This brings us again to the definition of violence and what forms can violence take. Psychological violence is commonly used to describe activities lacking physical aspects, but causing psychological damage to the victim. Similar in consequences is verbal violence and also cyber violence. However, the term cyber violence is usually used as a synonym for cyber bullying, therefore in a completely different connotation. Despite the evolution of the perception of violence, legal definition still remains the same. Therefore definitions based on violence as the only activity that can be under specific conditions regarded as terrorist acts have more difficult position in addressing cyber attacks. Cyber attacks in their very nature consist of breaking proprietary rights and causing material damage. Therefore if the definition includes damage to property as an activity possibly regarded as terrorist act, the definition can be easily applied on the cyber attacks as well.

[80] Oxford Dictionary, http://oxforddictionaries.com/definition/english/violence?q=violence (accessed on 21st January 2012)
[81] U.S. Government, *U.S. Code,*(U.S. Government), Title 18, Part I, Chapter I, paragraph 16, http://www.law.cornell.edu/uscode/text/18/16 (accessed on 21st January 2012)

This aspect of the definition is very important. Under this concept of definition of terrorism a terrorist sending an email would not be classified as an act of terrorism. The same applies to spreading information on the Internet. The most disputable case is WikiLeaks. The process of making potentially classified information public is sometimes labeled as cyber terrorism,[82] but it would not be so under the concept discussed here even if the motivation and goal of this action is in coherence with the definition.

Generally speaking, no supporting activities by terrorist groups, relying on the use of the Internet and computers, should be qualified as acts of terrorism. Stealing information, gathering intelligence about potential targets, spreading propaganda – neither of these actions would be considered as an act of terrorism. The term 'cyber terrorism' would only be used for such actions that would potentially endanger human lives or cause significant economic damage, provided that they fulfill all other aspects described in given definition.

Following chart describes the basis of each definition already analyzed.

Aspect / Definition	How is defined an act of terrorism?
U.S. Department of Defense	Calculated unlawful violence / threat
National Strategy for Combating Terrorism	Premeditated violence
Code of Federal Regulations	Unlawful use of force / violence
FBI	Violent / dangerous acts
Council of the E.U.	Extensive list
Russian	Violence, destruction / threat
Chinese	Violence, destruction or intimidation

Majority of the definition uses the term violence to define an act of terrorism. It would be very difficult to declare that cyber attack is an act of terrorism according to those definitions, even if all other criteria are met.

[82] Ewen MacAskill, *Julian Assange like a hi-tech terrorist, says Joe Biden,* (guardian.com: Washington, 2010), http://www.theguardian.com/media/2010/dec/19/assange-high-tech-terrorist-biden (accessed on 13th February 2012)

6.6.1. Definitions of terrorism and cyber attacks

Having analyzed all aspects of listed definitions and having discussed possible problems when addressing cyber attacks, it is time to decide whether particular definition is wide enough to address cyber attacks.

6.6.1.1. Definition from National Strategy for Combating Terrorism

Cyber terrorism would comply in terms of motivation stated in this definition. Nevertheless, this definition states noncombatant targets as possible victims of terrorist attacks. Cyber attacks would comply with this definition in some cases, but it limits possible attacks only to those aimed at noncombatant targets disregarding attacks causing substantial economical damage. Violence is again the basis of this definition. As already discussed, cyber attacks do not include physical violence and therefore cyber attacks would not be regarded as acts of terrorism according to this definition.

6.6.1.2. Definition from Code of Federal Regulations

Cyber attacks would comply with this definition in terms of motivation, goals and also possible targets, since this definition states property as possible target of terrorist attacks. Nevertheless, this definition is again based on the violence and use of force, thus including the element of physical power, which is not present in the cyber attacks. Despite the fact that this definition leaves more space in term of possible targets and motivation, it is limited by stating only use of force or violence can be regarded as acts of terrorism when meeting other features of the definition. Therefore according to this definition it would be difficult to classify cyber attack as an act of terrorism.

6.6.1.3. Definition of FBI

This definition is very detailed in certain aspects. Cyber attacks would comply with majority of aspects, like motivation and possible targets. Activities stated as possible acts of terrorism do not include only violence, but also act dangerous to human life. Cyber attacks can be dangerous to human life, thus being coherent with all aspects of this definition. Cyber attacks could be regarded as terrorist acts according to this definition. However, only cyber attacks design to cause causalities could be regarded as acts of terrorism, not attacks designed to cause significant damage.

6.6.1.4. Definition of the Council of the European Union

This explicit definition contains only several points that can be hardly met by cyber attack. Points (a), (b), (c), (e) and (f) cannot be committed by cyber attacks or only under specific conditions. But other features of this definition easily fit for cyber attacks, since this definition focuses mainly on the motivation and possible consequences of terrorist attacks, not on the form of an attack. Vast majority of cyber attacks as defined in this paper would comply with the point (d), possibly also (g) and (h). Generally speaking cyber attacks would be considered as acts of terrorism according to this definition.

6.6.1.5. Russian Definition of Terrorism

This definition states violence and destruction as possible acts of terrorism, when meeting other conditions set by this definition. Since cyber attacks would comply with the destruction or threatening to destroy, there is no obstacle to regard cyber attacks as acts of terrorism when other conditions are met according to this definition.

6.6.1.6. Chinese definition of terrorism

This definition leaves open space for possible kinds of attacks that can be regarded as terrorist attacks as it states "…and other means" in the beginning of the definition. Cyber attacks would easily meet other criteria stated by the definition, like motivation and goals. Therefore it is possible to say that cyber attacks would be regarded as acts of terrorism according to this definition if other conditions are met.

6.7. Conclusion

In this chapter, several definitions of terrorism were analyzed from different perspectives. Common features of these definitions, their discrepancies and also their potential to create a basis for globally accepted definition of terrorism were discussed. However, the most important part of this analysis regarding the subject of this dissertation is the answer for the question, whether current American definitions are valid for cyber terrorism as well.

Despite the fact that majority of definitions have common features, their theoretical background and legislative environment create so many potential discrepancies that they are not compatible. The extensional approach is not the most transparent and

comprehensible from the theoretical perspective. However, it is the most likely concept to success on the global level. European Union and its common definition is a good example of using this method. It is logical to expect that in the near future, only particular actions will be considered as acts of terrorism on the global level, thus slowly but truly making a list of such actions in accordance with the extensional approach.

Finally, first chapter proved that not all definitions are applicable on cyber attacks. The usage of term violence is the most visible reason for this result. Violence in its legal meaning necessarily includes physical contact between the victim and the attacker. This aspect is out of question in cyber space. Despite the fact that the common understanding of the term violence has evolved and it is nowadays used also to describe psychological attacks or virtual attacks against integrity of an individual, legal explanation of this term has remained intact so far. This "gap" can be found also in the most important American definition – the definition from the Code of Federal Regulations. This creates potential uncertainty in terms of effective fight against terrorists in cyber space. Nevertheless, it is necessary to admit that despite this finding the current legal environment in the U.S. presents many other means that can be used against terrorist despite this "gap" in the definition. No matter how it would be interesting, it is not the subject of this dissertation to analyze current American legal system in terms of competences given to the security forces to fight terrorism.

The initial hypothesis proved to be partially correct despite the fact that the impacts may not be as serious as thought, since some American definitions are applicable on cyber terrorism and other legal measures were implemented to strengthen the security forces in the fight against terrorism in all realms, even in cyber space.

7. Terrorism – prevailing threat?

7.1. Introduction

Terrorism as a threat to national security has been part of national security strategy of many countries, including the U.S., for many years. Despite this fact the importance of the terrorism threat dramatically changed after the attacks from 9/11, when terrorist proved that the threat is real also for the countries without strong separatist movements or other national problems as religious fundamentalism or ethnic intolerance. The severity of the terrorist threat was also highlighted by attacks in Spain. The political consequences of these attacks showed how strong influence the threat of terrorist attacks may have on the population, particularly on the elections. National strategies addressed this threat in many different ways. In some countries new security measures were implemented in order to lower the risk of terrorist attacks. In some cases the security measures were rather controversial as some people argument that the sacrifice of freedom and privacy in the name of increased security was inappropriate to the risk. National security strategies are based on classified information and there are many different influences shaping them. But is it possible to actually find an empirical evidence that the threat of terrorism is still real? Can it be stated that the war against terror was successful or failed? Are new types of terrorists attacks likely to occur? These are some of the questions this paper aims to answer.

7.2. Theoretical background

Deductive logic will be used to prove or reject formulated hypothesis. Deductive logic is a reasoning method which formulates logically certain conclusion as a logical result based on more general statements – premises.[83]

The first premise considers the threat terrorism presents. If the premise that this threat is influenced by the number of active terrorist organizations and by the number of their members is accepted, a decrease in those numbers would logically lead to the statement

[83] František Ochrana, *Metodologie vědy* (Prague: Karolinum, 2009), chapters 3.1 and 5.1

that the terrorist threat is diminishing. This premise is focusing mostly on the quantitative aspect. It does not take into consideration qualitative differences between particular terrorist organizations. The reason is that the threat of a terrorist attack in general does not influence the result terrorist attack might have. The attacks in London might have resulted only in few injured people if the bombs failed to explode, but the threat of the attack in the underground system remains unchanged. Another argument against accepting this premise is the location factor. This premise does not make any qualitative differences between terrorist organizations from Asia or from Europe. The following analyses is based on reports created by U.S. governmental offices or similar reports created by the E.U. Let's presume that terrorist organizations not perceived as a potential threat would not be listed in such important documents. Another argument in favor of this premise is the global world. Terrorist organization based in Afghanistan was able to execute surprise attack in New York in 2001. This is a precedent strongly in favor of the premise stating that every terrorist organization is potential threat disregarding its location. There are other factors influencing the threat terrorism presents, like security measures, but for the purpose of this analysis the general premise will be accepted that the number of active terrorist organizations directly influences the threat terrorism presents.

The first hypothesis for this analysis will therefore be following: The threat of terrorism remains unchanged as the number of terrorist groups has not decreased. Another approach to determine the terrorist threat is based on terrorist attacks. As it is possible that the attacks are committed by individuals without any affiliation to existing terrorist groups, the result of previous analysis would not reflect their activities. The focus will be on the number of terrorist attacks in the previous years on a global level. The second hypothesis is: The threat of terrorism remains unchanged as the number of terrorist attacks has not decreased. To determine the threat particularly for the U.S., the hypothesis will be applied also on the number of terrorist attacks aimed at American targets.

The second premise answers the question, why the terrorists should seek new types of attacks. The key to the success of terrorist attack is the element of surprise. As in the asymmetrical warfare, it is practically impossible to create completely secure environment.

Potential risks are assessed and relevant security measures are implemented. On the other hand terrorists chose the most surprising target and type of attack in order to avoid strong security measures while still inflicting maximum damage. This asymmetry was well described in the statement published by IRA after their unsuccessful attack on the life of Prime Minister Margaret Thatcher in 1984: "You have to be lucky all the time. We only have to be lucky once."[84] Therefore not only the repeating of the same attacks will lead to lower efficiency because of improved security measures, but also the impact on the public will be lower than that of the first attack. The security standards at the airports all over the world after 9/11 can be regarded as an example of reactive security measures. Also repetitive events tend to have lower attention of the public. On the general bases the premise that decreasing effectiveness of attacks will force terrorists to use a different type of attacks or to choose different targets is acceptable.

The third hypothesis will therefore be as follows: Terrorists are forced to seek new types of attacks if the success rate of terrorist attacks decreases. It is necessary to mention that in the case of this hypothesis the number of terrorist attacks will have to be considered as well. The reason is that the number of committed terrorist attacks influences the success rate. If the security forces manage to discover the plot to commit the terrorist attack before it takes place, it will not enter the statistics relevant for the success rate.

7.2.1. Methodology for statistical analysis

Statistical methods will be used in this paper in order to attempt to forecast the trends of analyzed data in the future years. The results could possibly influence the rejection or confirmation of the hypothesis based on the forecasted values. Statistical software will be used when analyzing data on number of terrorist attacks. The aim of this analysis is to prove the hypothesis that there is a trend in number of terrorist attacks. Basic comparison of numbers in previous years is not sufficient for the forecast, only statistical analysis of the time series can provide well-founded arguments for these assumptions.

[84] Lindsay Clutterbuck, *Terrorists Have to Be Lucky Once; Targets, Every Time,* (rand.org, 2008), http://www.rand.org/blog/2008/11/terrorists-have-to-be-lucky-once-targets-every-time.html (accessed on 9th October 2012)

Statistical tests will be performed to reject the hypothesis that analyzed data are random and therefore any further analysis of potential trend will have no results or results with little significance. Testrand software will be used to perform this analysis. Five basic statistical tests will be conducted to confirm or reject the hypothesis: Signs of difference test, Turning points test, Kendall coefficient test, Spearman coefficient test and Median test. The data in the tests is compared to the normal distribution characteristics and based on the result the hypothesis of independently and identically distributed data is confirmed or rejected. The Signs of difference test, Spearman coefficient test and Kendall coefficient test are used to determine whether the tested data has increasing or decreasing tendency – such tendency leads to the rejection of the random data. The Turning points test analyses if the data is not suspiciously too smooth or too unbalanced. The Median test analyses if the data has too many matches and is therefore suspiciously too rough, or has too little matches and is therefore too smooth.

The Signs of difference statistic is counted according to following formula:

$$T = \frac{\mathrm{k} - (\mathrm{n} - 1)}{\sqrt{\frac{\mathrm{n} + 1}{12}}}$$

T stands for the final value of test statistic, k stands for the number of signs of difference (positive) and n stands for the number of data.

Turning points test is counted according to following formula:

$$T = \frac{\mathrm{r} - \frac{2(\mathrm{n} - 2)}{3}}{\sqrt{\frac{16\mathrm{n} - 29}{90}}}$$

T stands for the final value of test statistic, *r* stands for the total number of turning points and *n* stands for the number of data.

Kendall coefficient test statistic is counted according to following formula, which uses the value of Kendall coefficient (τ):

$$T = \frac{\tau}{\sqrt{\frac{2(2n+5)}{9n(n-1)}}}$$

$$\tau = \frac{4v}{n(n-1)} - 1, \tau \in \langle -1; 1 \rangle$$

T stands for the final value of test statistic, *n* stands for the number of data and *v* is a constant based on analyzed data.

Spearman coefficient test statistic is counted according to following formula, which uses the value of Spearman coefficient (ρ):

$$T = \rho\sqrt{n-1}$$

$$\rho = 1 - \frac{6}{n(n^2-1)} \cdot \sum_{i=1}^{n} (i - q_i)^2$$

T stands for the final value of test statistic, *n* stands for the number of data, *q* stands for the order value and *i* stands for the order.

Median test statistic is counted according to following formula:

$$T = \frac{u - (m+1)}{\sqrt{\frac{m(m-1)}{2m-1}}}$$

T stands for the final value of test statistic, *u* is the total number of data groups separated by a median line, *m* stands for the number of these groups above (below) median line.

SAS Learning Edition and Gretl will be used for the statistical analysis. Standard regression cannot be used as the data belongs to a time series. An attempt will be made to identify the trend and use it to predict numbers for the coming years. Standard 95% level of probability will be used for these forecasts. The quality of identified trends will be discussed in the same time. R squared (R^2) will be used to evaluate the quality of identified trends:

$$R^2 = \frac{\sum(\hat{Y} - \bar{Y})^2}{\sum(Y - \bar{Y})^2}$$

Y stands for the actual value observed in the given year, $\hat{Y}$ represents the value fitted (or predicted for the future) by the trend model, $\bar{Y}$ represents the mean of the data. R^2, the coefficient of determination, indicates how well the trend line explains the data. R^2 has the value from 0 to 1[85] when 1 signifies a perfect fit – 100% of the data is explained by the trend line and there are no residuals.

Gretl software is used to determine the level of autocorrelation of given data. Tested data is copied and moved on the time axis up to eight steps on the time line forward and correlation test is performed. Applied lag will be 8 years in maximum in our analysis. Applied method for autocorrelation analysis is the analysis of residuals when original data set is compared with adjusted data set with the lag of defined size (up to eight years in this analysis. Statistical significance of the autocorrelation is displayed on a chart with 95% level of confidence.

[85] Depending on the calculation and used regression, the value might be in some cases higher than 1 or even negative.

7.3. Number of known terrorist groups

The main goal of security measures is not to find all terrorists and sentence them, but to lower the probability of successful terrorist attack aimed against civilians of a given country. Secondary goal might be understood as a definite removal of the threat terrorism presents. Therefore the number of terrorist groups or members of terrorist groups does not determine the danger they present to the society, but can be regarded as an indirect indicator of the danger of terrorist attack.

Considering the global role of the U.S., many terrorist groups define their policy towards the U.S. and American policy in the region as a part of their raison d'être. Accepting certain level of error, let's assume that the tendency in the number of terrorist groups globally can be used to assess potential danger for the U.S. It is true that it is not necessary to eliminate members of a terrorist group to remove the threat they present – it is sufficient to force them out of the region so they are not threat anymore. But in global world, this presumption is not valid anymore, especially if considering other means of terrorism, which do not require physical presence of attackers in the place of attack, like cyber terrorism. Specific position of the U.S. in this case is highlighted in charts describing the number of terrorist attacks against Americans abroad (see below). American foreign policy requires diplomatic and also military presence in many locations all over the world. The security of such personnel significantly differs from the situation in the U.S. The security measures in American facilities in such countries might be sufficient, but the general level of security measures in the country might be significantly lower. This increases the probability of a successful terrorist attack because of two reasons – insufficient security measures implemented by local administrations, presence of possible terrorist targets in the region where particular terrorist group is active. Such group might have not the potential to strike in the U.S., but attacking an American target is consistent enough with their strategy.

It is difficult to determine how to define an active terrorist organization which still presents danger to the society. One characteristic might be the number of active members or the

number of attacks in the past. However, even an inactive terrorist group might be considered as potential risk because of their political goals that may inspire others.

EU every year publishes list of persons and organizations regarded as terrorists or terrorist organization according to Common Position 2001/931/CFSP. This list is updated several times per year and it has the form of a Council Decision. Taking into consideration the regular updates including the removal of persons and organizations from the list, it is logical to assume that this list contains only terrorist organizations presenting a real threat. The following table presents the number of enlisted organizations from Council Decisions published every year since 2002. The chart is based on the list published at the beginning of a given year.[86]

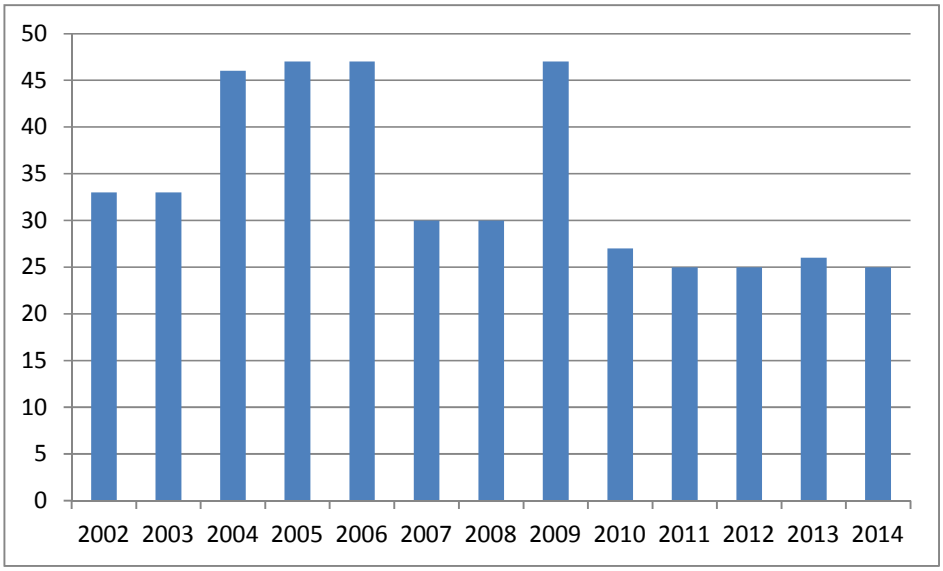


Chart 4 - Number of terrorist organizations as stated in EU Council Decisions in respective years

[86] The list is updated several times a year in a form of Council Common Position updating Common Position 2001/931/CFSP on the application of specific measures to combat terrorism. All Council Common Positions addressing the terrorist groups can be accessed here: http://eur-lex.europa.eu/search.html?instInvStatus=ALL&text=updating%20Common%20Position%202001/931/CFSP&qid=1404759945433&DTC=false&DTS_DOM=ALL&textScope=ti-te&type=advanced&SUBDOM_INIT=ALL_ALL&DTS_SUBDOM=ALL_ALL (accessed on 12th April 2014)

The Office of the Coordinator for Counterterrorism under the U.S. Department of State publishes the list of foreign terrorist organizations according to the definition of terrorism in Immigration and Nationality Act.

“"Foreign Terrorist Organizations" is compiled every 2 years by the Office of the Coordinator for Counterterrorism. Under the statute, this report is subject to judicial review. The Secretary of State makes designations following an exhaustive interagency effort. The designations expire in two years unless renewed. The law also allows groups to be added at any time following a decision by the Secretary, in consultation with the Attorney General and the Secretary of the Treasury.”[87] This factsheet has been published every year since 2001. Numbers of listed entities during the last ten years are shown in following chart.[88]

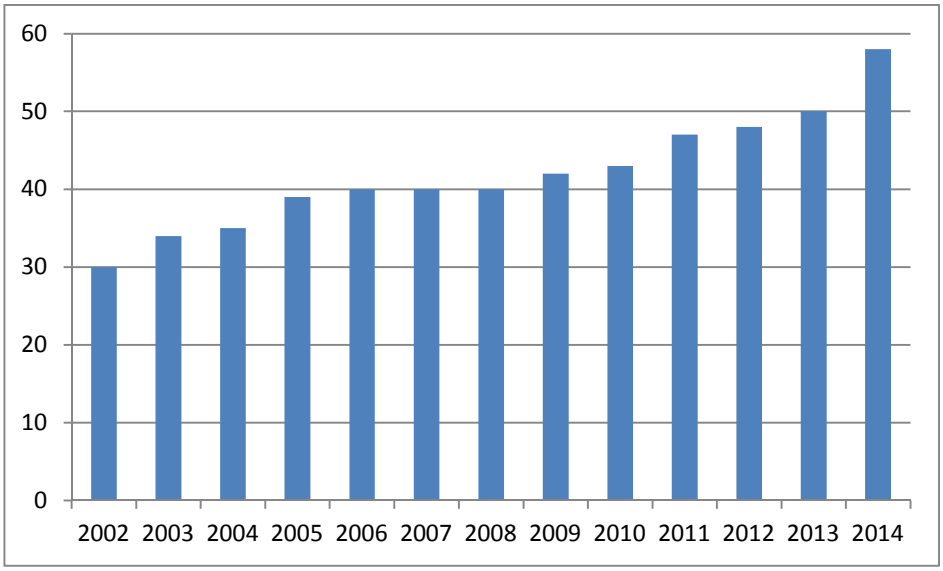


Chart 5 – Number of terrorist organizations published in Foreign Terrorist Organizations by Office of the Coordinator for Counterterrorism in respective years

It is interesting to compare the lists of terrorist organizations published in the U.S. and in the EU. Discrepancies probably arise from different interests in foreign policy and also from different criteria when selecting organizations for the list. Similar tendency can be observed

[87] “Foreign Terrorist Organizations”, official site of the U.S. Department of State, http://www.state.gov/j/ct/rls/other/des/123085.htm (accessed 28th April 2014)
[88] Ibid

in both lists up to the year 2009. There are exceptional years 2007 and 2008 in the EU list, but the number of terrorist organizations rises in 2009 back to the level comparable with the list published in the U.S. In 2010, the number of terrorist organizations listed by the EU decreased to the level around 25 and it has been oscillating around this number in the following years. On the other hand, the number of listed terrorist organizations in the U.S. has been continuously increasing. The list shows that the organizations listed after 2009 are mainly Islamist fundamentalists. Despite the discrepancies between the American and European lists of terrorist organizations, it is possible to say that both charts present evidence that terrorist organizations present a serious threat to American security, because their number has not significantly decreased.

Another approach to state the number of terrorist groups that present potential threat is to analyze their activities. Following chart is based on data from Global Terrorism Database.[89] It shows the number of active terrorist organizations all over the world. For the purpose of this analysis an active terrorist organization will be defined as an organization that committed at least one attack in the given year. Actual numbers of terrorist organizations in given year may differ due to the fact that in some cases it was impossible to identify the organization and the attack was labeled as unknown.

[89] The National Consortium for the Study of Terrorism and Responses to Terrorism (START) is a university-based (University of Maryland) research and education center that manages database used in this research. Database was downloaded on 16th May 2014 from following webpage: http://www.start.umd.edu/gtd/

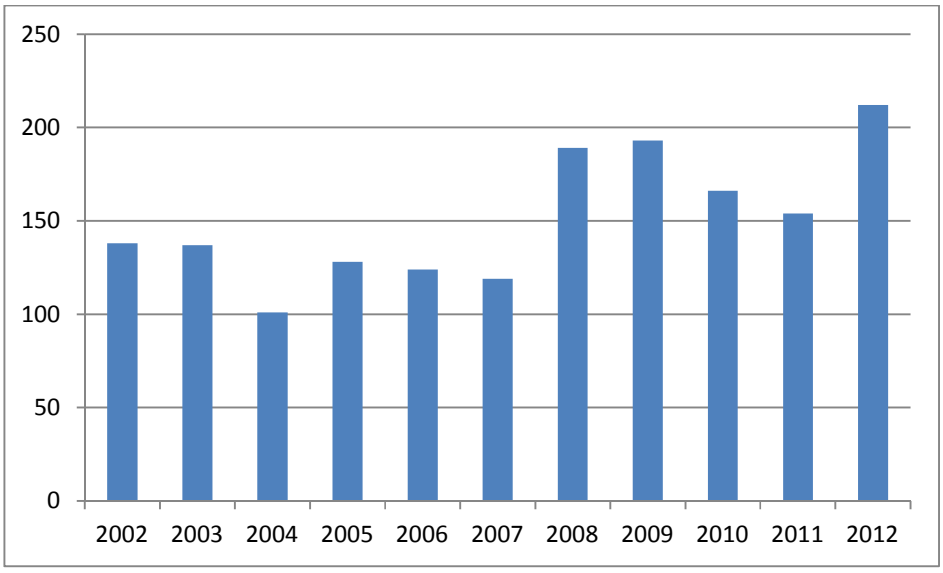


Chart 6 - Number of globally active terrorist organizations based on START data

Due to the specific global role of the U.S. in the world, there is a difference between terrorist groups active there and terrorist groups attacking American targets. Let's take the situation in Iraq or in Afghanistan as an example. Acts of terrorism against American soldiers or allied forces (ergo against American interests) are very numerous, but this kind of terrorist attacks does not present as dangerous threat as terrorist attacks committed in the U.S. from several reasons. Firstly, the political effect of such actions is limited as these actions have been happening since the beginning of the war on terror. Secondly, the social and economic impact is very limited as the attacks takes place outside of the U.S. The following chart show the number of terrorist groups actively attacking American targets in the U.S. and on the global level.

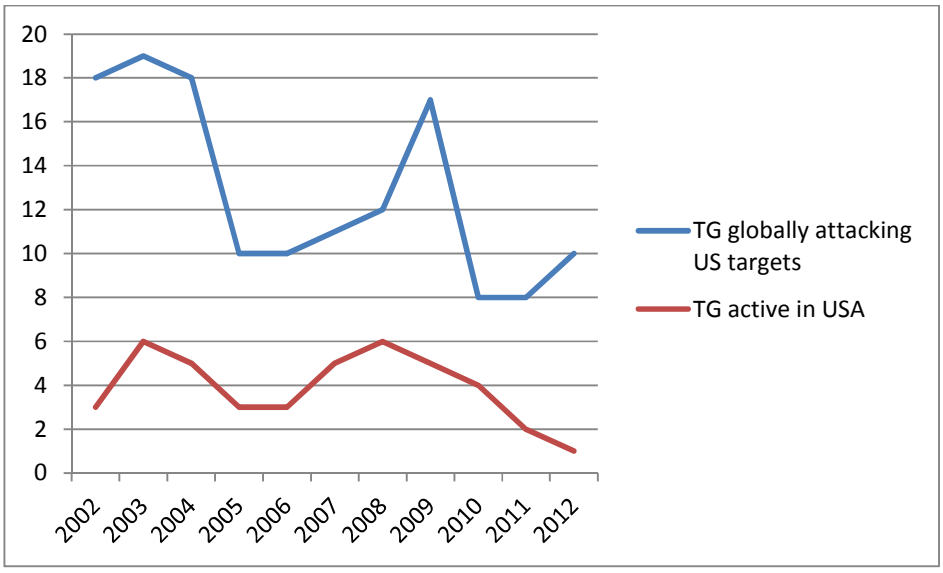


Chart 7 - Active terrorist organizations in the U.S. and on a global level based on START data

It is visible that the number of terrorist groups committing terrorist attacks in the U.S. has been constantly decreasing. This might be thanks to the implemented security measures. But it is necessary to consider the fact that the number of active terrorist groups influences the number of committed attacks only partially. Terrorist attacks can be committed by individuals with no affiliation with existing terrorist groups or the identification of responsible terrorist group is not possible. On the other hand the number of terrorist organization attacking American targets on the global level is increasing. This tendency might be related to the rise of extremism in North African countries where the dramatic changes of the Arab spring influenced also the attitude towards some organizations considered as terrorist groups in the Western countries.

Combining the data for terrorist attacks against American targets both in the U.S. and on the global level with the number of listed terrorist organizations in the U.S. results in the following chart. It is visible that in the last years the number of terrorist attacks against American targets all over the world is lower than the number of terrorist organizations as defined by the Office of the Coordinator for Counterterrorism under the U.S. Department of State. This proves that terrorist organizations listed by the Office of the Coordinator for Counterterrorism under the U.S. Department of State does not have to commit terrorist attacks against American targets to be on the list. It is not necessary to perform detailed

analysis of the attacks as in the years 2009, 2010 and 2011 the total number of terrorist attacks against American targets is lower that the number of listed terrorist organizations. To increase the validity of this hypothesis a detailed analysis of the attacks and listed terrorist organizations is needed, but for the purpose of this analysis it is sufficient to state that in three consecutive years the list of terrorist organization included terrorist organizations which had not committed any terrorist attack in the given or previous year.

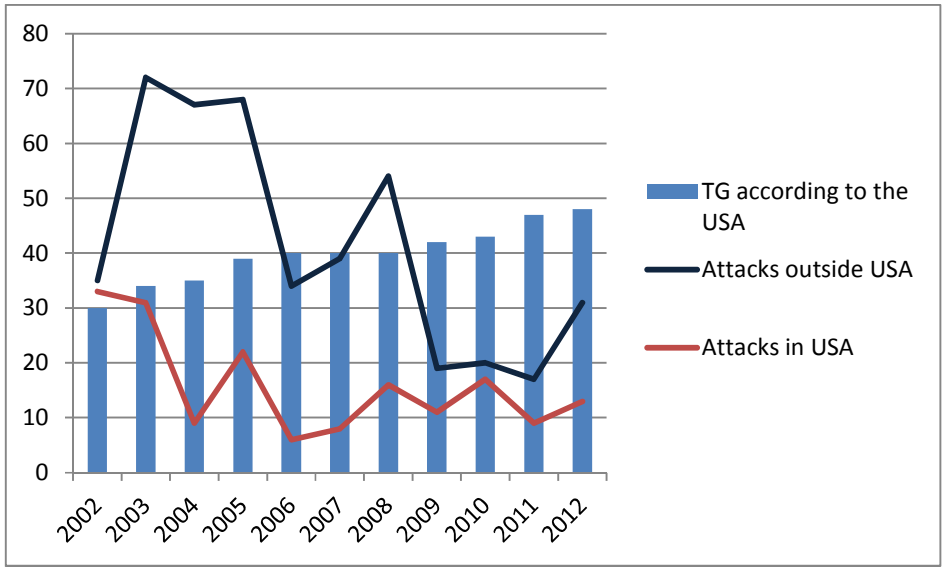


Chart 8 – Comparison of terrorist groups and number of terrorist attacks based on START data

Presented data supports the hypothesis, that current security measures and political pressure did not influence the number of terrorist organizations characterized as potentially dangerous to American security and American interests as listed by the Office of the Coordinator for Counterterrorism. However, this analysis does not state that taken measures have not diminished the probability of terrorist attack in U.S. or abroad. If the premise, that existence of terrorist organization presents a potential threat to the U.S., disregarding the probability of successful attack, is accepted, the threat has remained unchanged and according to data provided by the Office of the Coordinator for Counterterrorism has even risen.

7.4. Analysis of terrorist attacks

The previous part has showed that security measures have not seriously influenced the number of active terrorist groups. However, it is still possible that the risk terrorist organizations present have been diminished. Following charts describe the number of terrorist attacks in the world since 1970. The focus will be not only on the general number of terrorist attacks, but also on the terrorist attacks committed in the U.S. and on the terrorist attacks against American targets. This will allow us to compare the global trend of terrorist attacks with trends of terrorist attacks against American targets. Moreover, the comparison with trend in attacks against American targets will be used to find out whether the counter terrorist measures on national level are efficient.

The trend in success rate of terrorist attacks will be analyzed to prove or reject the hypothesis that the success rates in attacks against American targets and against targets in the U.S. are decreasing. The analysis is based on the START data (see above).

7.4.1. Terrorist attacks on a global level

Following chart displays the number of terrorist attacks committed around the world since 1970. The data set is complete up to the year 2012 with the exception of 1993. Data for the year 1993 were lost and all attempts to retrieve them have been unsuccessful.[90]

[90] Explanation regarding data consistency: "…cases from 1993 were lost prior to receiving the data from PGIS (Pinkerton Global Intelligence Service). Efforts thus far have been unsuccessful in fully recovering the 1993 data…" presented on the START web page: http://www.start.umd.edu/gtd/using-gtd/ (accessed 16th May 2014)

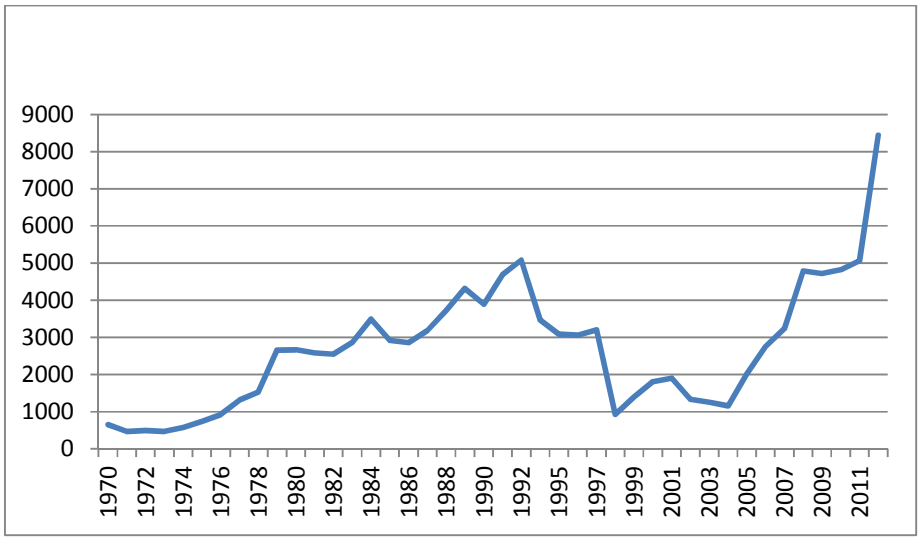


Chart 9 – Number of terrorist attacks in the world based on START data

If used data is limited only to the terrorist attacks committed by identified terrorist groups and the results are compared with the total number, the result is the following chart:

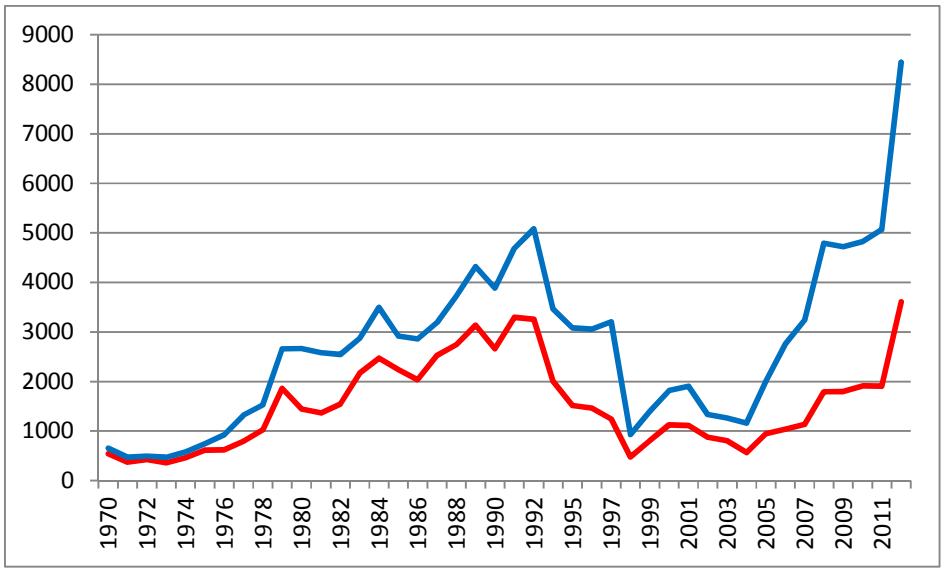


Chart 10 – Number of terrorist attacks committed by known and unknown perpetrators based on START data

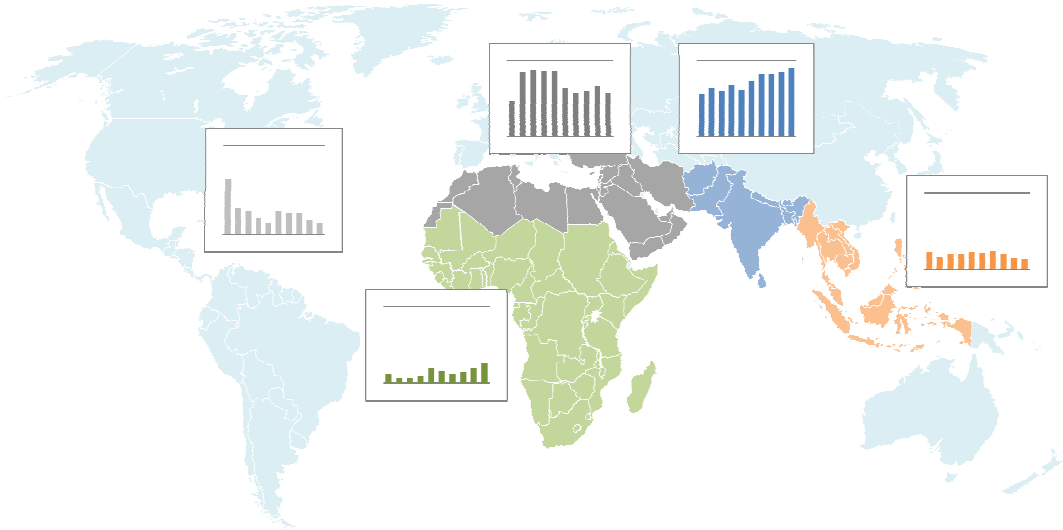
The chart displays a continuous increase in the number of terrorist attacks committed on the global level during the last decade. Similar trend can be observed in the case of attacks where the perpetrators were identified. The difference between the number of attacks committed by unknown attackers and attacks committed by known terrorist groups has been significantly increasing since 2004. From this year the number of attacks committed

by unknown perpetrators has always reached at least 50%. This is a very interesting fact since the basic principle of terrorism is to spread terror and panic among the public in order to pursue the goals of given terrorist party. The political aspect of terrorist groups cannot be realized without spreading the information about the identity and political affiliation of the attackers. Terrorist groups either claim the responsibility or the investigation leads to the identification of the perpetrators. Claiming the responsibility for the attacks can be motivated by different reasons - competition among terrorists, signaling strength, religious motivations or political motivations.[91] Two trends will be further analyzed – the increase in the number of terrorist attacks and the increase in the number of attacks committed by unknown perpetrators.

7.4.1.1. Analysis of the increase in the number of terrorist attacks

The increase started in 2005 when the number of terrorist attack doubled when compared to the year 2004. This increase corresponds to political events in Iraq. The war ended in 2003 and the democratization process culminated in the elections which took place in 2005. To validate the hypothesis that the increase in the number of terrorist attacks is related to changes in the Middle East region, particularly in Iraq, the percentage distribution of attacks among regions will be analyzed. If the hypothesis is correct, the share of the regions Middle East and North Africa is dominant in years following 2004. For this analysis the total number of committed attacks is considered disregarding the identification of the perpetrators.

[91] Austin Lee Wright, *Why do terrorists claim credit?* (Austin: The University of Texas at Austin, B.A. Government, Sociology, May 2009), pages 3-8, http://scholar.princeton.edu/austinlw/files/Wright_Paper.pdf (accessed 14th March 2014)



Picture 5 – Distribution of terrorist attacks among region based on START data

The picture above displays the regional distribution of terrorist attacks. The limit was set to 6%. Only four regions had the number of terrorist attacks over 6% between the years 2003 and 2012. The charts are showing the percentage share of the region from 0% to 50%. The Middle East and North Africa together with South Asia have the highest share of terrorist attacks in the last years. Regarding our hypothesis, the picture suggests that the increase in terrorist attacks between the years 2004 and 2007 was truly caused by the increased number of attacks in the Middle East and North Africa. The second phase of the increase from the year 2008 onwards seems to be related to the increase in the size of the share of terrorist attacks in the South Asia region. This increase is also supported by slight change in the size of the share of Sub-Saharan Africa reaching 13% in the year 2012. Further analysis of the Middle East and North Africa region shows that the number of terrorist attacks in this region between the years 2004 and 2012 is driven mainly by Iraq, as shows the following chart.

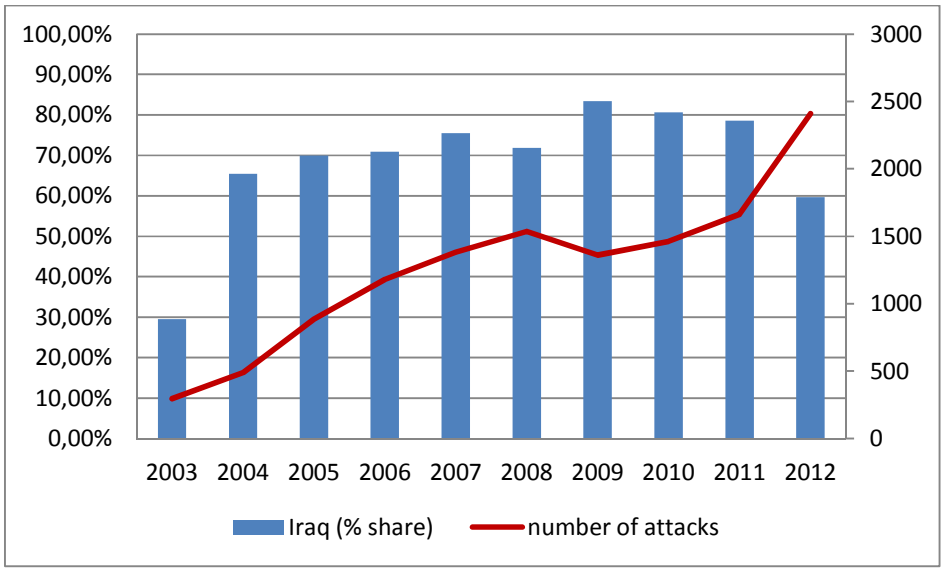


Chart 11 – Number of terrorist attacks in the region compared to the share of Iraq, based on START data

This chart shows the percentage of terrorist attacks committed in Iraq together with the total number of terrorist attacks committed in the region. Iraq increases the size of the percentage share between the years 2004 and 2007 even if the total number of attacks increases. Therefore the hypothesis that the increase in terrorist attacks between years 2004 and 2007 was caused by increased activity of terrorist groups in Iraq is confirmed. Further research is needed to determine if the main reason was the political unrest, attempts to further destabilize the country or to take revenge on American soldiers.

The increase in the total number of terrorist attacks between years 2007 and 2012 seems to be generated mainly by the increase in the South Asia region. This suggests that the unrest in Afghanistan became more violent in those years. Nevertheless, further analysis of available data showed that the increase cannot be attributed so easily to the situation in Afghanistan. India, Pakistan and Afghanistan have the largest share of terrorist attacks in this region. Together they create more than 75% of all attacks in the region, 98% in the year 2012. However, it is difficult to determine the main factor as their shares seem to oscillate around the same percentage. Following chart displays the percentage share of the three countries together with the evolution of total number of terrorist attacks in this region.

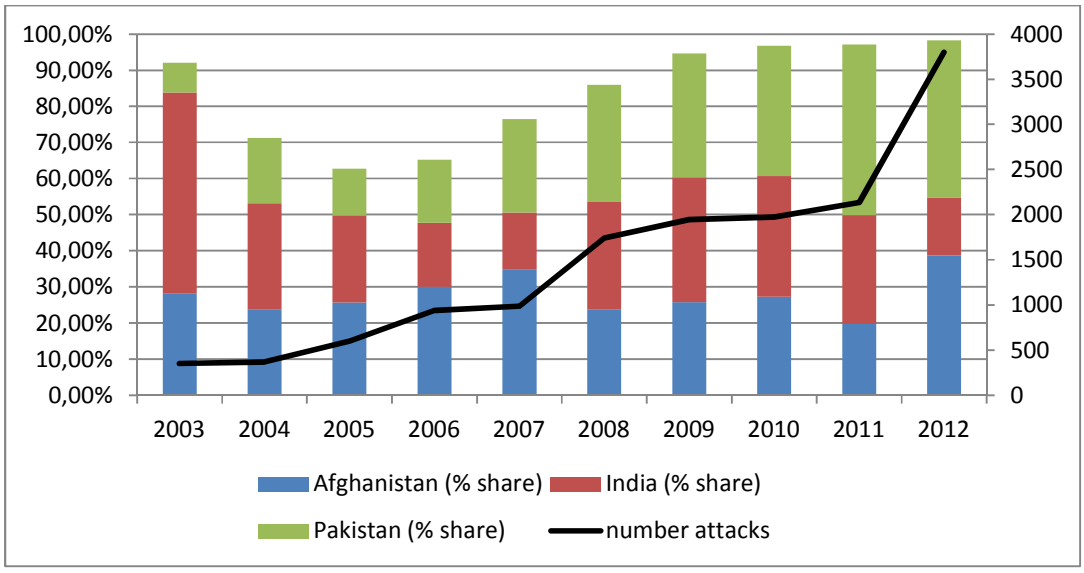


Chart 12 – Number of terrorist attacks in South Asia region and share of particular countries in the region based on START data

The share of Pakistan has dramatically increased after the year 2005. The size of the Indian share was oscillating around 27%, the same counts for Afghanistan. Despite the increase in the size of Pakistani share, the average size of the share for all three countries is almost the same – from 27% to 28%. This suggests that the increase in number of terrorist attacks in this region after the year 2007 is equally caused by the increase in the number of terrorist attacks in Afghanistan, India and in Pakistan. Terrorist attacks in Afghanistan can be related to the unstable political situation. Further analysis is needed to determine the reasons behind the increase in the number of terrorist attacks in Pakistan and in India. This research will be more complicate in Pakistan, since approximately 80% of committed terrorist attacks in 2012 were done by unknown perpetrators. Large part of the attacks in India in 2012 was committed by the Maoist groups, especially in the regions neighboring Bangladesh. Again, further research is needed to determine the reasons behind terrorist attacks in India. Original hypothesis that the number of terrorist attacks committed in this region can be attributed mainly to Afghanistan can be rejected. Clearly not only Afghanistan has major influence on the total number of terrorist attacks, but also India and Pakistan influence the total number of terrorist attacks committed in this region.

7.4.1.2. Analysis of the increase in the number of attacks committed by unidentified perpetrators

Following chart displays the percentage of unidentified terrorist attacks on a global level combined with the number of terrorist attacks.

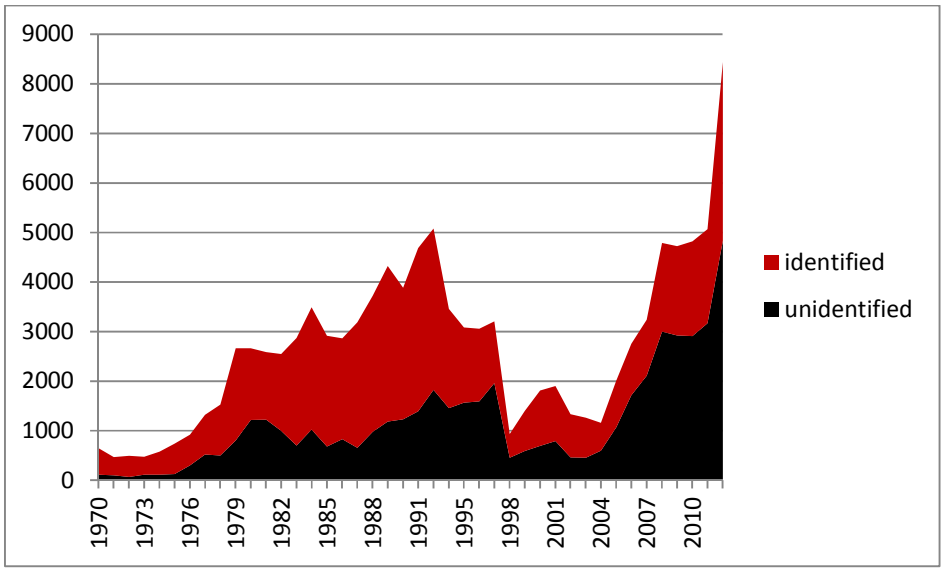


Chart 13 – Number of terrorist attacks committed by known and unknown perpetrators based on START data

The increase in the number of unidentified attacks correlates with the total number of terrorist attacks. The increase in the number of unidentified terrorist attacks started in the same period as the increase in the total number of terrorist attacks. Nevertheless, since 2004 the share of unidentified attacks remains approximately the same - around 60%. Further analysis shows that since 2004 almost 75% of unidentified attacks are committed in South Asia, the Middle East and North Africa regions. South Asia gained the upper hand in 2012 when the size of the share was almost 46% while the size of the Middle East share decreased to 33% - the lowest share since 2004. Since 2004 three countries were having combined share of more than 75% - Iraq, Pakistan and Afghanistan. Iraq had traditionally the largest share till 2012 when Pakistan slightly took the lead, as shows the following chart:

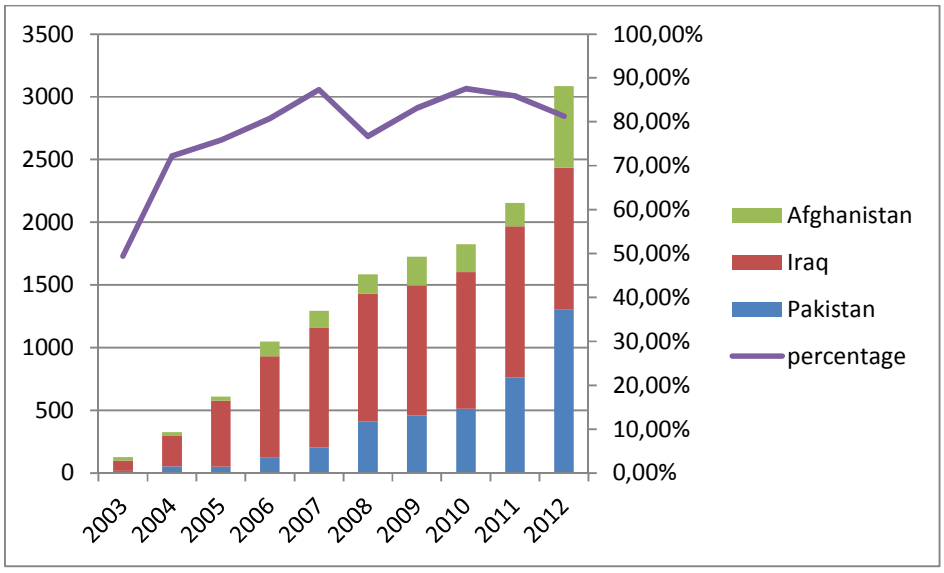


Chart 14 – Number of terrorist attacks committed by unknown perpetrators with the share of particular countries based on START data

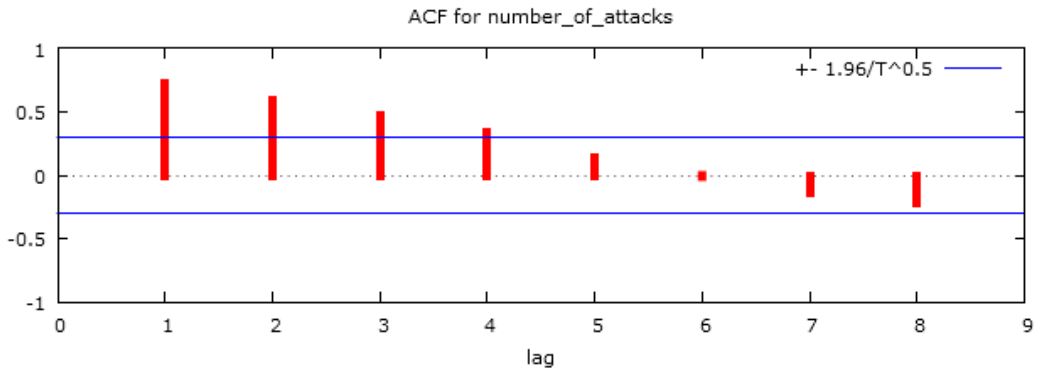
Further research is needed to determine the reasons why unidentified attacks occur in such a large number in these states while the same states generate the increase in the number of terrorist attacks.

7.4.1.3. Statistical analysis of terrorist attacks committed on a global level

The series describe a very disturbing fact – the number of committed terrorist attacks all over the world increased by 800% between 2004 and 2012. More than 8 000 terrorist attacks were committed in the year 2012, which is the highest number ever recorded in the START database.

Tests to determine the independency of the data rejected the hypothesis that the data are random and therefore there is no trend to be identified. Only the Spearman coefficient test and the Kendall coefficient test did not reject the hypothesis that the data is random. Given the definition of these tests a conclusion was reached that it is impossible to determine if the data has shown an increasing or decreasing tendency. However, this result does not confirm the hypothesis that the data is random, but it indicates that the trend will be more difficult to identify.

The autocorrelation test using the Gretl software is positive, as the following picture displays. This mean that the number of attacks in year *t* is influenced by the number of attacks in previous years – in this case the influence is statistically significant 4 years in the past (t-4). The conclusion that terrorism is contagious is supported also by the findings of Luis de la Corte Ibáñez.[92]



Picture 6 – Gretl software output showing autocorrelation factor values for the number of terrorist attacks

The timeline has at least two peaks, where the second one is not yet closed by a decrease. Linear model and 95% confidence level for the predictions will be used. The trend line does not seem to have any seasonal factor, so Winter's method will not be used, but the stepwise autoregressive process. The following chart displays the actual values together with the model and forecast for five consecutive years:

[92] Luis de la Corte Ibáñez, *Logika terorismu* (Prague: Academia, 2009), page 82

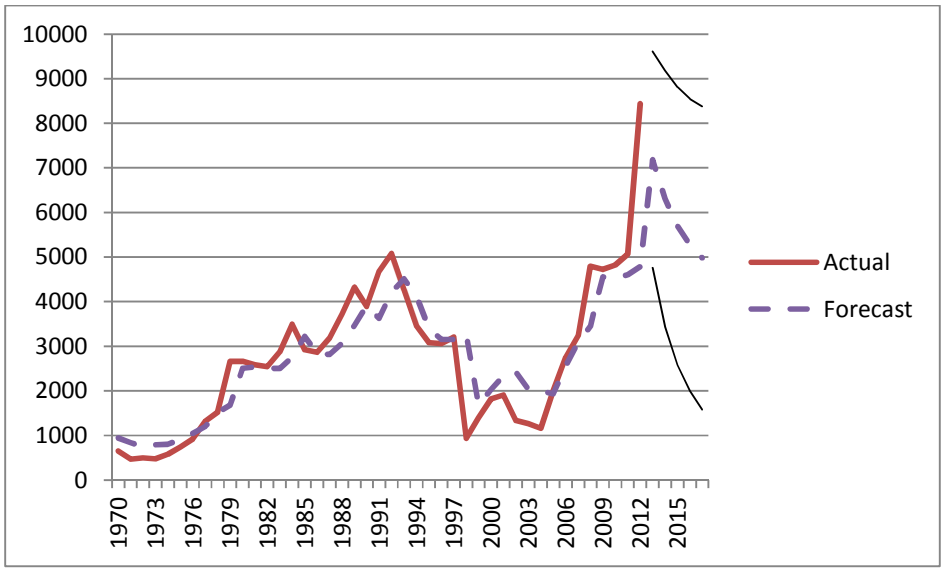


Chart 15 – Actual and forecasted number of terrorist attacks based on SAS software output

The displayed model has the value of R^2 equal to 0,75. Despite the fact that the model explains 75% of the value, the forecast for 5 years shows very wide spread of possible values within the confidence level. Nevertheless, the calculated model predicts decreasing trend in the number of terrorist attacks on the global level in the next five years. Possible explanation is that the decrease in the number of terrorist attacks which followed the first major peak in 1993 should occur in the near future from the statistical perspective. Statistical analysis showed that the number of terrorist attacks in the given year is influence by the number of attacks committed in last four years.

7.4.1.4. Summary

The analysis of terrorist attacks committed on a global level proved that the number has significantly increased since 2004. As the number of terrorist attacks raised the share of attacks committed by unknown perpetrators. Further analysis identified two periods within this increase. The first one was from the year 2004 till 2007. During this time, the increase in the number of terrorist attacks was caused by the intensified violence in Iraq. Iraq made up around 70% of all terrorist attacks committed in the region. The increase in the share corresponded to the raise of the number of terrorist attacks committed in the region. Since 2007, the share of Iraq remained the same. Therefore the further increase in the number of terrorist attacks had a different reason. Further analyses showed that this augmentation in

the number of attacks since 2007 was caused by the higher frequency of terrorist attacks in South Asia. Pakistan, Afghanistan and India. It is possible to state that Pakistan and Afghanistan had the strongest influence on the raise in the number of terrorist attacks during the second period of the increase. Whereas the reasons behind the elevation of the number of attacks in Afghanistan can be related to current unstable situation, further analysis is needed to determine the reasons for the increase of violence in Pakistan.

Surprisingly the increase in the number of terrorist attacks committed by unknown perpetrators is related to the countries causing the dramatic raise in the number of terrorist attacks. Again, this change was caused mainly by Iraq. Since 2011 the share of Pakistan raised as well as the share of Afghanistan. This tendency is very interesting as the influence of terrorist groups generally claim the responsibility for the attacks to strengthen their influence and to achieve their goals. It is possible that terrorist groups behind these attacks in particular regions (e.g. Baghdad) have such a reputation that they do not need to officially claim the responsibility. Another possible explanation might be that these attacks are made by individuals without affiliation to any terrorist groups. It is necessary to include also the option that this might be caused by problems in the definition of terrorism or by discrepancies in data, but this seems rather improbable. Further analysis is needed to identify the motivation of terrorists for not claiming the responsibility.

Statistical analysis of the data indicated that the data is internally depended (previous values influence consecutive values) and therefore creates a time series. The test of autocorrelation showed that the number of terrorist attacks committed in given year is influenced by the number of attacks in previous four years. This seems to be logical as the success of terrorists in their activities motivates them to continue. The R^2 value for the model is relatively high – 0,75. The model suggests that a decrease in the number of terrorist attacks in the near future can be expected. However, the confidence level boarders are very wide – the spread is almost 6000 attacks. This means that the number of attacks might dramatically decrease in the next year and then increase again. A more sophisticated model is needed to improve the statistical strength of the prediction.

7.4.2. Terrorist attacks against American targets

When focusing on the terrorist attacks against American targets, it is necessary to distinguish terrorist attacks committed in the U.S. and terrorist attacks against American targets in the rest of the world. There are several reasons for this approach. Firstly, American government has direct control over the security measures implemented in the U.S. in order to fight terrorism and to reduce the probability of successful terrorist attacks. Secondly, the number of attacks against American targets committed in the rest of the world illustrates the risks for American citizens and personnel related to the American foreign policy. Moreover, the American government has no direct control over security measures implemented in foreign countries which are protecting also American citizens. Official facilities located outside the U.S. within the authority of the U.S. State Department or the Department of Defense are exceptional, as the security measures implemented to protect these facilities are either partly (e.g. security checkpoints in the streets close to American embassies) or completely (e.g. internal security procedures in American military bases located abroad) under American control. The following chart shows the number of terrorist attacks committed against American targets both in the U.S. and in the rest of the world:

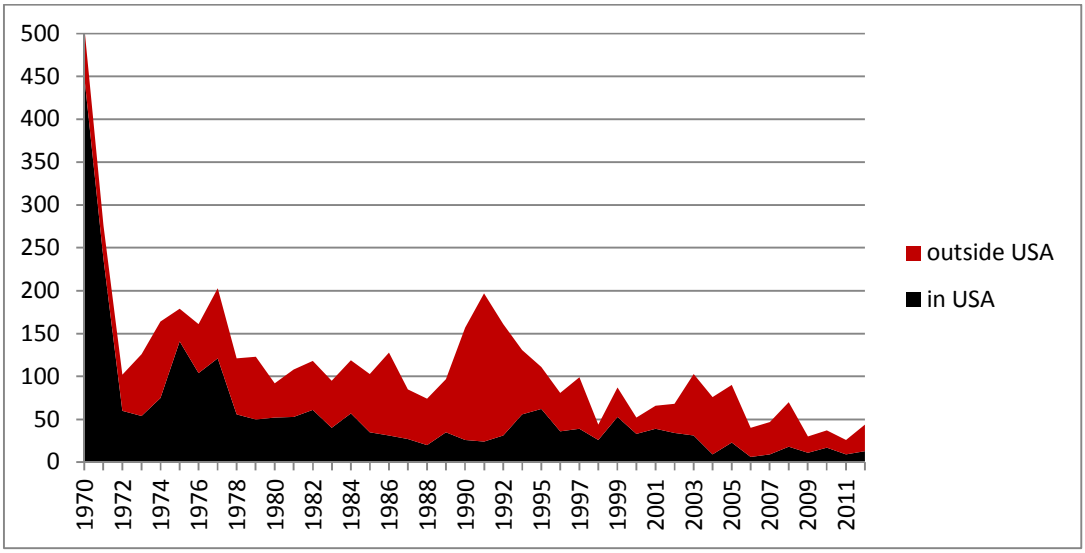


Chart 16 – Number of terrorist attacks against American targets committed in the U.S. and in the rest of the world, based on START data

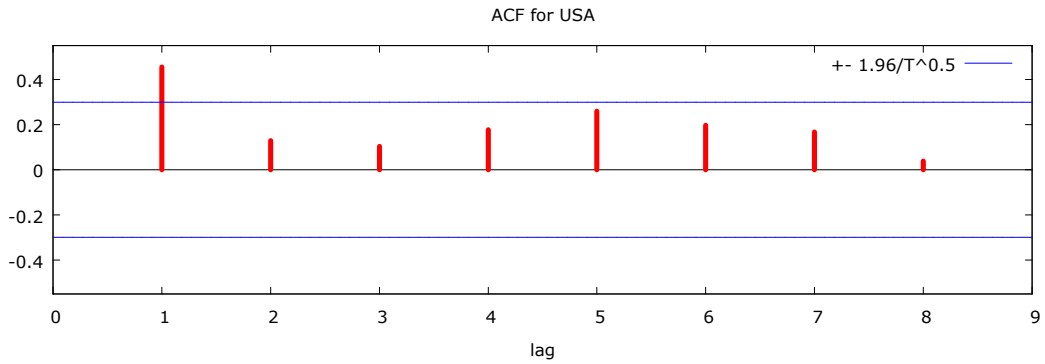
It is visible that the number of terrorist attacks committed against Americans is oscillating around 100 attacks per year. There are several peaks influencing the average value, which is 114. The peak in the 90s can be explained by the Gulf War and by the presence of American soldiers and personnel abroad. The diversity of perpetrators and locations of terrorist attacks in the 70s suggest that there were more reasons motivating the terrorist attacks and a further analysis is needed to determine the motivation of the terrorists.

The chart shows that in the 70s the vast majority of terrorist attacks against American targets took place in the U.S. However, since then the number of the attacks against American targets committed outside the U.S. has been higher than the number of attacks committed in the U.S. There are exceptional years (e.g. 1975 or 1999), but the general trend seems to be clear – terrorist attacked American targets mainly outside the U.S. The engagement of American personnel abroad as a part of American foreign policy increases the risk of terrorist attacks as the security measures implemented to protect American citizens and personnel abroad are not sufficient to completely avoid the risk of terrorist attacks, which is higher than in the U.S. The peaks in the number of attacks against the American targets outside U.S. corresponds to military actions conducted by the U.S. in abroad. For instance, in 1991 the increase in the number of attacks corresponds to the first Gulf War, the increase in the years 2001 – 2005 can be related to the wars in Afghanistan and in Iraq. Analyzed data suggests that implemented security measures in the U.S. helped to reduce the number of terrorist attacks as the number decreased. Despite the decrease in the number of attacks committed in the U.S., the threat terrorist attacks present remains unchanged. The attacks are not so numerous, but their impact on the society is still very strong, as proved by the terrorist attack in Boston in 2013. The risk of terrorist attacks against American targets outside the U.S. remains the same; especially in countries that have not implemented any security measures against terrorism. The data suggest that the number of terrorist attacks committed against American targets is related to American military operations abroad. These actions incite terrorist actions against American targets in the location of the American actions and in the neighboring countries.

7.4.2.1. Statistical analysis of terrorist attacks targeting American targets

The first part of the analysis did not reject the hypothesis that analyzed data (number of terrorist attacks in the U.S.) are independent. All five tests of data independence did not reject the hypothesis that the data is random. Any further predictions for the number of terrorist attacks committed in the U.S. will have to consider this result. On the other hand, only two of the same tests for the number of attacks against American targets in the rest of the world did not reject the hypothesis that the data are random. The difference test and the Turning points test did not reject the hypothesis, but remaining three tests did. Further analysis should therefore respect these results and aspire to identify the decreasing trend indicated by the Spearman and the Kendall coefficient tests.

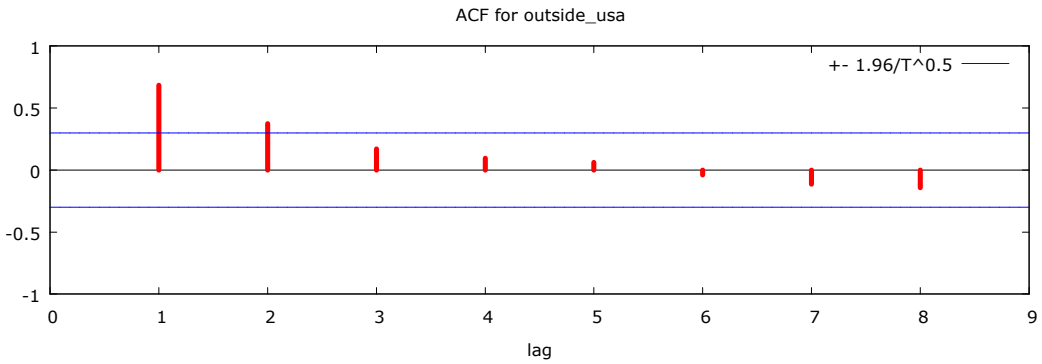
Autocorrelation test for the number of attacks committed in the U.S. using the Gretl software is positive for a one year lag, as following picture displays. This means that the number of attacks in year *t* is influenced by the number of attacks in previous years – in this case the influence is statistically significant 1 years in the past *(t-1)*.



Picture 7 - Gretl software output showing autocorrelation factor values for the number of terrorist attacks in the U.S.

Results of the same test for the number of attacks against American targets in the rest of the world is statistically significant for two years lag, as following picture displays. This mean

that the number of attacks in year *t* is influenced by the number of attacks in previous years – in this case the influence is statistically significant 2 years in the past *(t-2).*



Picture 8 - Gretl software output showing autocorrelation factor values for the number of terrorist attacks against American targets outside the U.S.

The following chart shows the actual values and forecast for years 2013 up to 2017 for the number of terrorist attacks in the U.S. and against Americans in the rest of the world. Displayed model for the number of terrorist attacks in the U.S. has the value of R^2 equal to 0,54; model of the number of attacks against Americans in the rest of the world has the value of R^2 equal to 0,51. For both models the quadratic method option was used.

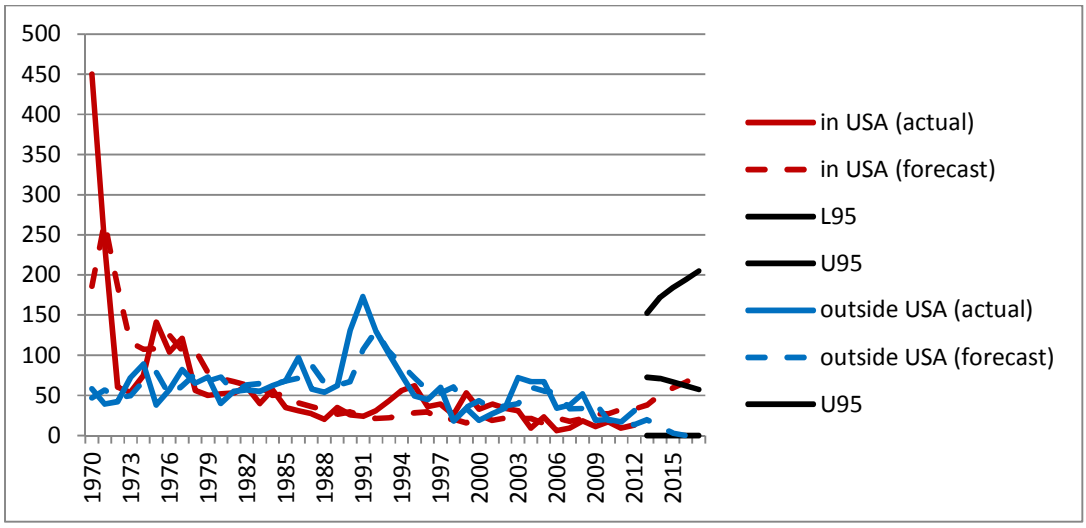


Chart 17 - Actual and forecasted number of terrorist attacks against American targets committed in the U.S. and in the rest of the world based on SAS software output

Despite the fact that the model explains approximately 50% of the value, the forecast for 5 years shows very wide spread of possible values within the confidence level. Nevertheless, calculated model predicts a decreasing trend in the number of terrorist attacks against American targets outside the U.S. On the other hand, the statistical model predicts that the number of terrorist attack committed in the U.S. should increase in the next five years.

7.4.2.2. Summary

The number of terrorist attacks against American targets has been relatively low in the last years. Despite the peak in the 90s, the number of attacks was decreasing and since 1996 has remained under 100 in total. The number of attacks committed in the U.S. is very low. The decrease actually started in 1999 with the exceptions of 2001 and 2005. It is possible to deduce that security measures implemented in the U.S. were successful as the number of attacks committed in the U.S. decreased. On the other hand it is important to say that the number of terrorist attacks committed in the U.S. was already low when compared to the total number of attacks in the world for the same years.

The number of terrorist attacks targeting Americans outside the U.S. can be related to American foreign policy. The increase in the 90s and in the 2003 corresponds to the military activities in Iraq and in the Middle East. Nevertheless, also the number of attacks against American targets outsider the U.S. was decreasing in the last years, remaining lower than 50 since 2008.

Statistical analysis did not reject the hypothesis that the number of terrorist attacks committed in the U.S. is independent. The results of the same tests for the number of attacks committed outside the U.S. were not so straightforward – only two tests did not reject the hypothesis. There is no doubt that these results are influenced by the low number of attacks against American targets. Autocorrelation tests showed that the number of attacks committed in the U.S. is influenced by the number of attacks in the last year. The number of attacks in the rest of the world is influenced by the number in the last two years.

The model for both analyzed data sets has very similar R^2 value – around 0,5. The model suggests that the number of attacks committed in the U.S. will increase in the following years, but the number of attacks in the rest of the world should decrease. Given the low quality of the model and the results of the random data sets these predictions are not statistically reliable.

7.4.3. Success rate of terrorist attacks

Important information is also the success rate of terrorist attacks. The hypothesis for this analysis is that if the success rate decreases, the terrorist might be more motivated to seek new tools and means to actually increase the success rate and to minimize the impact of newly implemented security measures.

Following chart shows the success rate of terrorist attacks on a global level, in the U.S. and against American targets in the rest of the world. The expectations are that the success rate of terrorist attacks on a global level is increasing, in the U.S. is decreasing and outside the U.S. attacking American targets is decreasing as well.

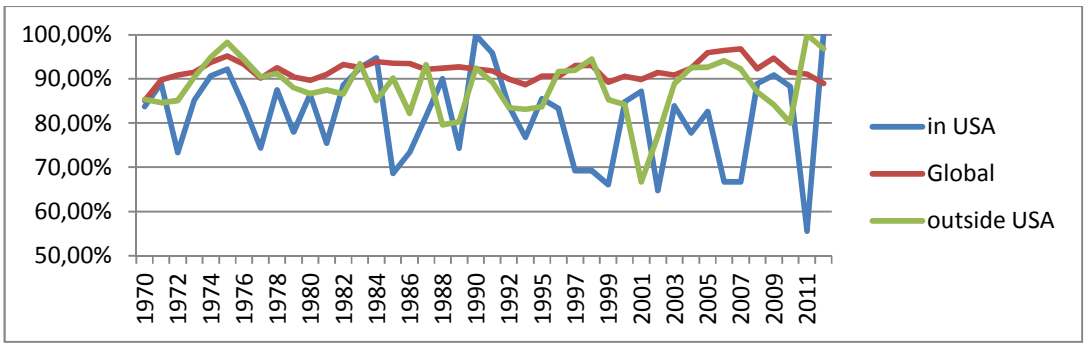


Chart 18 – Success rate of terrorist attacks, based on START data

The chart shows that the success rate of attacks against American targets disregarding the locality has a very wide spread. The success rate moves from 65% up to 100% in some years. The data suggests that the statistical model for prediction will be very difficult to identify. On the other hand the success rate of terrorist attacks on the global level oscillates around the average, which is 92%, with minimal differences. Another important factor

related to the success rate is the number of terrorist attacks (analyzed above). The spread of the success rate is influenced by a very low number of terrorist attacks in the U.S. and in the rest of the world attacking American targets. On the other hand, the high number of terrorist attacks on a global level smoothens the line of a terrorist attacks' success rate. The spread of the success rate values over the years suggests that the probability of terrorist attack' success is particular for every terrorist attack and it can hardly be related to previous events.

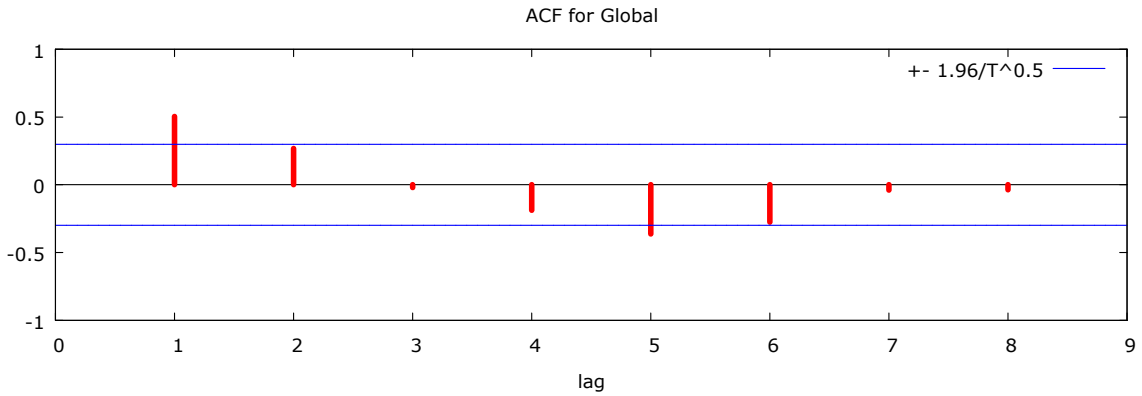
7.4.3.1. Statistical analysis of terrorist attacks' success rate

Visual analyses of the success rate suggested that the model will be very difficult to identify as the data seem to be independent. This possibility will be analyzed using the tests to reject the hypothesis that the analyzed data is independent. All three sets of data will be analyzed – success rate of terrorist attacks on a global level, success rate of terrorist attacks committed in the U.S. and success rate of terrorist attacks aimed at American targets outside the U.S.

Only two of the applied tests for the global terrorist attacks' success rate rejected the hypothesis that the data is independent – the Turning points test and the median test.
Three of five tests rejected the hypothesis of the independent data in the case of terrorist attacks in the U.S. success rate – the Turning points test, the Kendall coefficient tests and Spearman coefficient test. The results for the success rate of terrorist attacks committed outside the U.S. attacking American targets are in favor of the independent data hypothesis – only the Turning points test refuses the hypothesis. The results of the success rate data test were not definite. In some cases the results suggest that the data is more or less independent. These results have to be considered when commenting the forecast model.

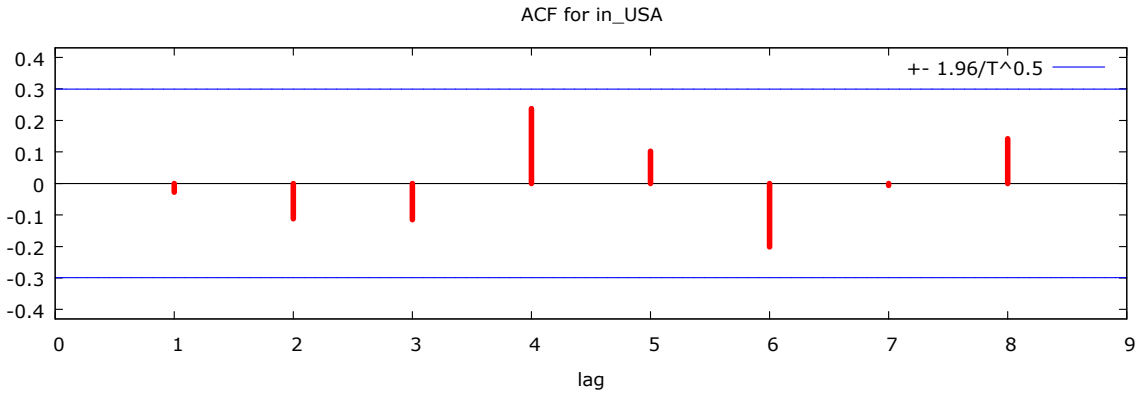
The autocorrelation test for the terrorist attacks' success rate on the global level using the Gretl software is positive for a one year lag, as the following picture shows. This means that the number of attacks in year *t* is influenced by the number of attacks in previous years – in this case the influence is statistically significant 1 years in the past *(t-1).* Surprisingly, the results suggest that the value in given year is also influenced in the fifth year lag *(t-5),* but in

this case negatively. This anomaly is another fact supporting the hypothesis of the independent data.



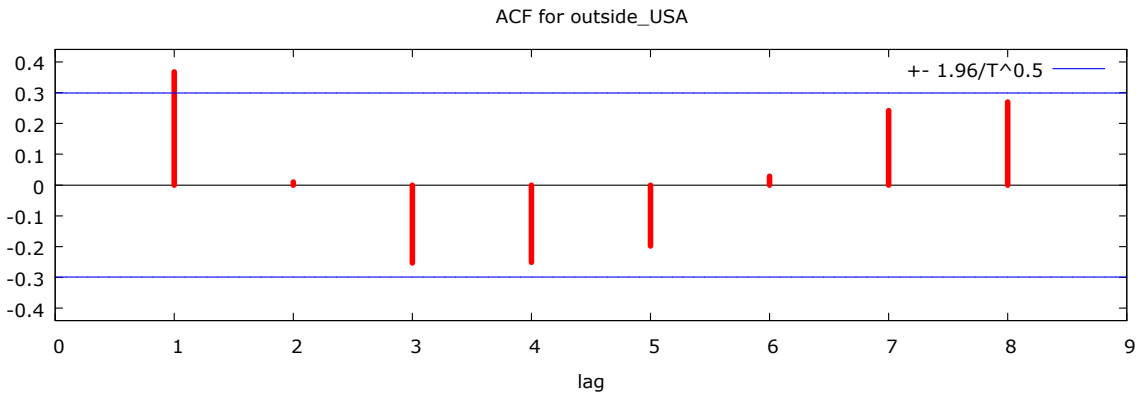
Picture 9 - Gretl software output showing autocorrelation factor values for the terrorist attacks' success rate

The autocorrelation test for the success rate of terrorist attacks committed in the U.S. is negative – there is no influence of the previous 8 years' values on the current value that would be statistically significant, as the following picture shows:



Picture 10 - Gretl software output showing autocorrelation factor values for the success rate of terrorist attacks' committed in the U.S.

The autocorrelation test for the success rate of terrorist attacks committed outside the U.S. aimed at American targets is positive for the first year lag *(t-1).* The results are displayed in following picture.



Picture 11 - Gretl software output showing autocorrelation factor values for the success rate of terrorist attacks against American targets outside the U.S.

The next picture shows the forecast for analyzed success rates. Displayed results are based on the time series analysis using constant degree of time trend model, which yielded the highest R^2 values. Nevertheless, the R^2 values for all observed success rates data are very low. This is partially caused by the random characteristic of the data identified in previous tests. The R^2 value for the success rate on the global value is 0,28; 0,04 is for the success rate of terrorist attacks committed in the U.S. and 0,29 for the success rate of terrorist attacks committed outside the U.S. aiming at American targets.

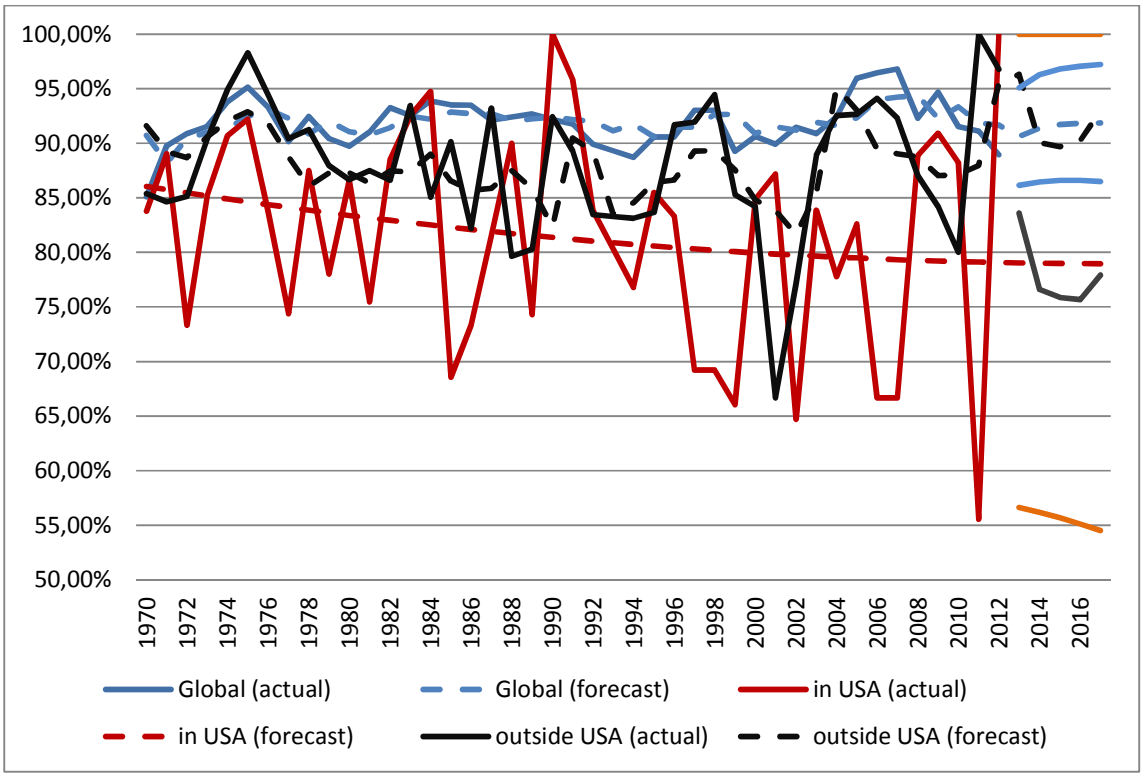


Chart 19 - Actual and forecasted number of terrorist attacks' success rates based on SAS software output

The chart shows that only the forecast for the success rate of terrorist attacks committed on a global level has reasonable spread of forecasted values within the confidence range corresponding to 95% confidence level. However, even in this case the model suggests spread between 87% and 97%. Given the low R^2 value, the forecast for the success rate of terrorist attacks on a global level addresses not even one third of the value. Despite the relatively low spread in forecasted confidence level boarders, the low R^2 values and spreads of boarders of confidence level in other analyzed data sets suggests that the data are independent (random) and any forecasts are not statistically significant. It would be necessary to create more complex model with additional variables to strengthen the predictions.

7.4.3.2. Summary

The chart showed that the success rate of terrorist attacks committed on a global level oscillated around the value 92%. On the other hand the success rates for attacks committed within the U.S. and those committed outside the U.S. targeting American targets have large

variety of values. The spread for theses two lines have been actually increasing in the last years. This is visible particularly for the line describing the success rate of attacks committed in the U.S. This characteristic of the data is related to the number of attacks actually determining the success rate of terrorist attacks. Since the global success rate is created by thousands of events, the line seems to be smoother as the principles of the big numbers apply. However, as the number of terrorist attacks committed in the U.S. and outside the U.S. targeting American targets was slowly decreasing, the success rate became unstable and the oscillation increased in size. The extreme difference between the subsequent years reached almost 45% for the attacks in the U.S. and 20% for the attacks committed outside the U.S. targeting American targets.

From statistical point of view, the data available for the three analyzed trend lines are independent and forecasted values have a very limited explanatory value. This leads us to a conclusion that the possible trend in the success rate of terrorist attacks cannot be identified with such a simple model. Any attempts to forecast future success rate of terrorist attacks will have to create a more sophisticated model with additional variables having direct influence on the number of terrorist attacks and on the success rate. This means that the probability of success of a terrorist attack must be judged on an individual level for every terrorist attack and it is impossible to determine whether the success rate has a decreasing or increasing tendency.

7.5. Conclusion

Analysis described in the previous pages proved that the threat of terrorism remains unchanged at least on the global level. The number of terrorist attacks significantly increased during the last decade and the number of active terrorist groups reached the highest peak in the year 2012. The number of terrorist attacks on the American official list increased, whereas the number of enlisted terrorist groups by the EU Commission remained the same in the last years. Despite the time discrepancy between the terrorist attacks' data and terrorist groups' data, the results are not contradictory. Even if considering the statistical model for the number of terrorist attacks on the global level was

statistically the strongest, the suggested decrease in the number of terrorist attacks might be relevant only to the countries that are actually responsible for the dramatic increase in the previous years (mainly Iraq and Pakistan). It is possible to state that on the global level the first two hypotheses can be confirmed – the threat of terrorism remains unchanged as the number of terrorist groups has not decreased and neither has decreased the number of terrorist attacks.

Although the war on terror is not successful on a global level, it brought some results for the U.S. It was discussed that the number of attacks again American targets has been fewer than 100. The number of terrorist attacks committed in the U.S. has dramatically decreased and so has the number of terrorist attacks committed in the rest of the world aimed at American targets. However, the correlation between occasional peaks in the number of terrorist attacks committed outside the U.S. with the American activities abroad based on American foreign policy occurred. This leads us to the conclusion that further American actions abroad, particularly in the Middle East and South Asia, might result in an increase in the number of terrorist attacks committed in respective countries aimed at American targets. It might also increase the risk of terrorist attacks in the U.S., but the data did not prove this relation. This leads us to the conclusion that American security measures have been successful in reducing the number of terrorist attacks in the U.S. However, the threat of terrorism remains unchanged. Despite the decrease in terrorist attacks against American targets that rejects the second hypothesis, the number of terrorist organizations listen by American authorities has kept increasing. Moreover it is necessary to consider the fact that the success of American security measures damages the data quality. Further research that would include the number of prepared terrorist attacks might increase the precision of the analysis. This conclusion is supported by the impact the Boston attack had on the public.

The success rate of terrorist attacks and its analysis showed that the data are independent and therefore it is impossible to identify a trend with statistical significance. The probability of success must be analyzed individually for every particular terrorist attack. This means that also any judgments based on the previous observations are not strong enough to confirm or reject the hypothesis that terrorists are forced to seek new types of attacks.

Nevertheless, it can be deducted that terrorists will seek new types of attacks in countries where their activities have diminished or have not been so successful. This applies also for the U.S. where the data proved that observed “traditional terrorist attacks” have been almost driven out of the U.S.

The application of statistical methods has revealed some important facts about the analyzed data. However, the identification of trends and creation of models proved to be very ineffective as the statistical strength of such models and predictions was very low. More sophisticated models with additional data might prove more useful to predict trends in such time series as is the number of terrorist attacks.

8. Options for terrorists – cyber weapons or WMD?

Previous chapters discussed that the most common form of attacks is more and more affected by security measures implemented in U.S. and in abroad. Terrorist organizations behind those attacks will need to change their tactics in order to achieve their goals, or they will have to completely modify their strategy. First of all it is necessary to define strategy of terrorist groups. Clear description of strategy is following:

"Terrorists attack civilians to coerce their governments into making political concessions."[93]

Nevertheless, even if accepting this description as a general definition of terrorists' strategy, it is necessary to acknowledge the existence of separate type of organizations targeting military personnel and facilities. Abrahms in his paper distinguishes two types of actions: terrorist actions and guerilla actions. Such distinction is needed with regard to particular definition of terrorism as discussed in the first chapter of this dissertation – some definitions states only civil targets, not military. However, majority of terrorist organizations do not focus solely on one type of actions. Despite the fact that one type might be more dominant, usually both types of activities are executed by given terrorist organizations. In other words terrorists' strategy is to create a situation similar to blackmailing - when making concession is an easier option for the government. Significant aspect of the strategy is its violent nature and the threat to society it presents. In democratic countries, terrorist group can give up the violent aspect of their strategy. For instance, IRA has made such a shift in strategy.[94] However, such change is not possible in non-democratic countries. But this process is influenced by many factors, including the nature of terrorist organization, their goals, etc. Possible changes in strategy could result in existence of new political parties in democratic countries or in creation of guerilla armies.

[93] Max Abrahms, *The Political Effectivness of Terrorism Revisited*, (Comparative Political Studies, 2012), http://cps.sagepub.com/content/45/3/366 , page 362 (accessed 21st November 2013)
[94] The Guardian, *Full Text: IRA Statement,* (theguardian.com, 2005), http://www.theguardian.com/politics/2005/jul/28/northernireland.devolution (accessed on 5th May 2013)

The aim of a strategy is to help to attain defined goals. The definition from Abrahms can be used:

"Terrorist groups possess two types of goals: process goals and outcome goals. Process goals are intended to sustain the group by securing financial support, attracting media attention, scuttling organization-threatening peace processes, or boosting membership and morale often by provoking government overreaction. The outcome goals of terrorists, by contrast, are their stated political ends, such as the realization of a Kurdish homeland, the removal of foreign bases from Greece, or the establishment of Islamism in India."[95]

Definitions of terrorism discussed in the first chapter of this dissertation describe only the outcome goals. Both types of goals need successful communication. Process goals require communication towards potential supporters or new members, outcome goals need communication about next actions, goals and aspiration. The communication related to process goals is very effective, since the number of terrorist organizations have not decreased, as described in the previous. Surprisingly, the communication related to outcome targets is not very successful. One of the reasons is the influence of mass media in targeted society and the level of journalism, because studies on media coverage find that actual political demands of terrorists are seldom stated[96]. It is usually the brutality of attacks, the number of victims or caused damage that makes the headlines. These communication problems might be another reason for terrorists to change their tactics.[97]

Current tactics of terrorist organizations can be derived from the types of committed attacks described in previous chapter. Most common type of attack in general would use explosives. Possibly suicide bomber or remotely triggered bomb in a crowded place or bus or other mean of transport. These types of attacks can be still very effective for fulfilling process goals, as martyrdom is one of the reasons why young people join terrorist

[95] Max Abrahms, *The Political Effectivness of Terrorism Revisited*, (Comparative Political Studies, 2012), http://cps.sagepub.com/content/45/3/366 , page 370 (accessed 21st November 2013)
[96] Ibid, 375
[97] Ibid, 391

organizations[98], but the ability to promote terrorists' goals is limited. This situation might motivate terrorists to change their tactics. These changes may involve new types of targets with lower protection or usage of more effective weapons.

8.1. Options for terrorists

It has been already said that it is improbable for currently active terrorist organizations to completely change their strategy. American security agencies have intensified their actions towards detecting terrorist cells and analyzing accessible information to prevent any potential terrorist attack. Given the fact that NSA and other agencies have access to huge amount of data provided by global companies like Facebook, Microsoft or Google under American legislation, the pressure on terrorist groups is increasing. Usage of a cell phone, sending an email or chatting through unencrypted web page might disclose their operations. There is sound evidence that terrorist groups all over the world were using modern technologies to exploit the potential cyber space offers.[99] However, the conditions have changed and the abilities of security agencies have significantly grown. It is reasonable to expect that terrorists will alter their behavior and processes to avoid being tracked via metadata in cyber space. Terrorist might acquire more sophisticated technologies like encrypted cell phones or specially secured computers. They also might return to messengers or other methods avoiding new security measures in cyber space. Of course the price for increased security would be lower flexibility – trained pigeon will not be detected by security agencies, but it is much slower than sending an email. Or they may take the risk, because the huge amount of data makes it difficult to analyze them and to find the crucial piece of information. This reaction to newly introduced security measures might be influenced by cultural aspects. In the same way, for instance, like the financial services in some Arab countries (Islamic banking).

---

98 Jeff Victoroff, *The Mind of the Terrorist: A Review and Critique of Psychological Approaches*, (The Journal of Conflict Resolution - SAGE, 2005), page 3-42, http://www.jstor.org/discover/10.2307/30045097?uid=3737856&uid=2129&uid=2&uid=70&uid=4&sid=21104625367781 (accessed on 5th May 2013)

99 John Rollins, *Terrorist Use of the Internet: Information Operations in Cyberspace,* (Congressional Research Service, 2011), http://fas.org/sgp/crs/terror/R41674.pdf, (accessed on 20th April 2013)

Terrorist organizations might change their way of communication, their organizational structure or the selection of targets to minimize the risk of being discovered before the attack takes place. But they can also try to find new means how to attack. This leads to widely discussed topic of the weapons of mass destruction and the probability of terrorists gaining access to them. Switching conventional explosives for chemical weapons would allow terrorists to be coherent with their current action schemes (e.g. suicide bombers), but would significantly increase the destructive potential of their attacks. The hypothesis of this chapter is that apart from weapons of mass destruction, terrorists might likely use cyber attacks to cause significant damage and to bypass newly introduced security measures, because of their availability. For the purpose of this dissertation following options will be taken into consideration: chemical, biological and nuclear weapons, cyber attack. These options are based on the premise that terrorist might use WMD in the future.[100] However, some authors believe that the usage of WMD by terrorists is not probable as it is not consistent with their ultimate goals in their region.[101] In the same time current terrorist attacks mean hijacking of transportation vehicle, suicide bomb attacks, bomb attacks and hostage taking. These types of terrorist attacks are based on records from terrorist attacks database.[102]

When analyzing options for the terrorists, two basic ways how terrorists can procure related weapons or equipment will be taken into consideration: internal and external. Internal option to acquire for instance biological weapons is to set up dedicated research facility with needed equipment, hire or educate qualified staff to conduct the research and in the end produce usable biological weapon. External option reflects that terrorists might find a way how to buy or steal final product (in our example biological weapon) or semi-finished product requiring only minimal adjustment before usage.

---

[100] US Army, *Terrorism and WMD in the Contemporary Operational Environment,* (US Tradoc, 2007), http://fas.org/irp/threat/terrorism/sup4.pdf (accessed 21st September 2014)

[101] James Forest, *Framework for Analyzing the Future Threat of WMD Terrorism,* (Journal of Strategic Security, 2012), http://scholarcommons.usf.edu/jss/vol5/iss4/9/, page 51-68 (accessed 24th September 2014); Steve Bowman, *Weapons of Mass Destruction: The Terrorist Threat,* (Congressional Research Service, 2002), http://fpc.state.gov/documents/organization/9184.pdf (accessed 24th September 2014)

[102] The National Consortium for the Study of Terrorism and Responses to Terrorism (START) is a university-based (University of Maryland) research and education center manages database used in this research. Database was downloaded on 16th May 2014 from following webpage: http://www.start.umd.edu/gtd/

8.2. Weapons of mass destruction

Despite the differences among biological, chemical and nuclear weapons, their similarities related to their procurement are numerous. Therefore they will be discussed as a one group.

8.2.1. Internal resources

Agreements on nonproliferation of weapons of mass destruction are influencing also the possibility to conduct independent research and manufacturing. Listed crucial components are monitored and their proliferation is either completely banned or under strict supervision both of national states and United Nations. This makes it very difficult to obtain needed material for nuclear weapons are nuclear radiation based bombs (e.g. dirty bombs). The supervision is very strict for all types of weapons of mass destruction, but it is extremely strict for nuclear weapons. Given the fact that even states have major difficulties to obtain all needed resources and conduct their own research in this field, it is possible to say that the probability of a terrorist group with sufficient resources conducts research and development of a nuclear weapon of their own is very close to zero because of needed materials, huge costs related to the research, needed time and necessary high profile scientists.

It is a similar case for the biological and chemical weapons. Nevertheless, since some chemical substances are largely used in agriculture or in other industries are also utilizable for manufacturing chemical weapons, it is easier to get access to them. Despite discussed obstacles and security measures, there is a precedent of a terrorist group manufacturing biological and chemical weapons.

In 1995 there was a terrorist attack in the Tokyo underground system executed by the sect Aum Shinrikyo. Terrorist used nerve gas sarin manufactured in their facilities. The gas wrapped in newspaper bombs was release by attackers penetrating these containers in five different underground trains. The attack claimed 12 lives and injured more than 5000 people. The attack might have had even more casualties had the manufacturing process be

more efficient. Produced gas was not pure enough and therefore could be smelt. This attack led after investigation to a big bust on the sect, which revealed some disturbing information.

The sect conducted research in biological and chemical weapons for seven years before the attack in Tokyo messing with much more dangerous substances than finally used sarin. The sect was successful in collecting needed financial and technical resources and even in hiring capable scientists. In the first phase the research focused on the botulin bacteria (Clostridium botulinium), the most toxic bacteria in the world. Despite numerous tests they performed, practical results were thankfully very poor. For example, in 1990 the sect used three trucks with specially designed sprayers to spread the bacteria around American base in Tokyo, but there were no casualties, neither injured. Same results had the attack with botulin on the royal wedding ceremony three years later. The sect then changed tactics and tried to spread spores of anthrax, but only few people were nauseated. Another attack using botulin was planned for 1995 in the Tokyo underground, but fortunately the attacker in the final moment sabotaged the action.

The Aum Shinrikyo case only demonstrates that even if all needed resources are available, it is very difficult to manufacture efficient biological or chemical weapon of mass destruction. For short illustration, the problem with biological weapons relate to the bacteria container, the mean of dissemination, the weather conditions during the attack, speed of the carrier, time of exposure to the sun, etc. All these factors may critically influence the result of the attack, which is exactly what happened to the Aum shinrikyo.[103]

8.2.2. External resources

Terrorist groups might seek to acquire prepared weapons of mass destruction without their own research. It might not be weapons in the final state, like a missile with chemical warhead, but just the critical part, in this case the warhead. The fear of terrorists having weapons of mass destruction was very particular during the transition of Soviet Union in

[103] Tom Mangold, Jeff Goldber, *A mnoho lidí zemřelo...pravda o biologických válkách,* (Themis: Praha, 2001), pages 359 - 375

the 90s. Nowadays it is again a strong topic especially with regard to terrorist groups supported by states and civil unrest in countries in possession of such weapons. Following table lists states knowingly in possession of weapons of mass destruction according to a report for Congress:[104]

Country	Nuclear Weapons Capability	Biological Weapons Capability	Chemical Weapons Capability
Algeria		research	suspected
China	yes	likely	suspected
Egypt		research	likely
France	yes		
India	yes		yes
Iran	research	likely	yes
Israel	yes	research	likely
Kazakhstan			suspected
Myanmar			suspected
North Korea	yes	likely	yes
Pakistan	yes		likely
Russia	yes	suspected	yes
Saudi Arabia			suspected
South Africa			suspected
South Korea			suspected
Sudan			suspected
Syria		research	yes
Taiwan			likely
United Kingdom	yes		
United States	yes		yes
Vietnam			likely

Table 4 – Overview of Proliferation States[105]

It is visible from the table above that terrorists do not have many possibilities where to get weapons of mass destruction. Nevertheless, recent civic unrests in countries in possession weapons of mass destruction (Egypt, Syria) raised serious concerns about the possibility of

[104] Paul K. Kerr, *Nuclear, Biological, and Chemical Weapons and Missiles: Status and Trends,* (Congressoinal Research Service, 2008), page 23, http://fas.org/sgp/crs/nuke/RL30699.pdf (accessed 5th May 2012)
[105] Ibid

terrorist groups taking advantage of momentary instability and take possession of chemical or biological weapons.

8.3. Conclusion

The probability of terrorist group successfully conducting research and manufacturing in order to obtain usable equivalent of a weapon of mass destruction is very low. Nuclear weapons are out of reach of terrorist group research capabilities. It has been very difficult for states to successfully conduct such research and it is almost impossible for terrorist groups. The difficulties related to biological weapons' development are so numerous that it is similar to the nuclear weapons – the probability of successful research and manufacturing process conducted by terrorist organization is close to zero. The obstacles for chemical weapons are less numerous, but still critical.

Given the needed effort and resources, it is much more probable that terrorists have been searching a way how to get access to ready-to-use weapon of mass destruction or usable equivalent from states in possession of weapons of mass destruction. Terrorists might hope to negotiate the supply with states more or less supporting certain terrorist groups or to make use of chaos and unrest in countries in possession of weapons of mass destruction and seize them by force.

Despite the fact that the external resources options' probability has risen recently due to the events in Syria and northern Africa during the Arab spring, the probability is rather low as all states are well aware of this problem. Hopefully the security measures and international political pressure will prevent the proliferation of weapons of mass destruction to terrorists. However, it is important not to forget that only limited number of terrorist group is able to operate in the region of Syria and Northern Africa. Therefore the option of using external resources to acquire these weapons is limited. Other terrorist groups cannot hope even for the low probability and have to seek other options.

8.4. Dangers in cyber space

The usage of cyber space combined with the increased role of modern technologies in our lives has been accompanied by the rise in the number of negative events. Some of these events were unintentional, for example software malfunctions or errors disrupting the desired usage of the device. Other events were intentional in the form of a cybercrime or hacktivism. The intentional events perceived negatively can be classified as cyber attacks, if the broader definition of this term is applied. Types of cyber attacks can range from malicious software collecting sensitive data to complex viruses destroying hardware or gaining control over critical infrastructure putting thousands of people at risk.

The aim of this chapter is to present basic types of tools and schemes used by perpetrators in cyber space to illustrate the existing dangers.

8.4.1. Consequences of cyber attacks

Internet serves its users in many ways. You can share data, access remote databases, control connected systems, purchase goods, offer services and much more. These different activities may all become the target of an intruder or a terrorist. Such attacks require a different approach and have different impacts.

In thrillers the worst scenarios usually involve the intruder completely controlling the targeted system, usually a missile silo or other crucial systems. Theoretically, it is not impossible for such situations to occur in real life. The Trojan horse was already mentioned before. The Trojan horse, installed in an important system, can grant the intruder access to the system. If it is some student's PC, the consequences are not so grave as if it is a system controlling the traffic at an airport. Gaining access to such systems may lead either to controlling the system according to the attacker's goals, or just to observe and gather further information from the inside. Examples stated above correspond to list from book called Maximum Security, where are stated several examples of intrusion as follows:

- The intruder gains access and nothing more (being defined as simple entry: entry that is unauthorized on a network that requires at minimum a login ad password.

- The intruder gains access and destroys, corrupts, or otherwise alters data.
- The intruder gains access and seizes control of a compartmentalized portion of system or the whole system, perhaps denying access even to privileged users.
- The intruder does not gain access, but instead forges messages from your system.
- The intruder does not gain access, but instead implements malicious procedures that cause the network to fail, reboot, hang or otherwise manifest an inoperable condition, either permanently or temporarily.[106]

8.4.2. Cyber attacks tools and schemes

Tools and schemes used by perpetrators to achieve their goals in cyber space will be briefly described. The motivation of their actions may differ as well as their goals, but the tools they use remain the same with few exceptions. There are special schemes like phishing, road apples or social engineering that can be used for different purposes, but the process does not change. There are different views on the classification of some of the tools, but since the aim of this part is to illustrate the possibilities cyber space offers to perpetrators, discrepancies among some approaches will not be considered. The lists of tools and activities do not claim to be definite, but they should be sufficient to cover the major dangers present in cyber space.

8.4.2.1. Tools

Viruses can seriously damage the system it attacks, but is not controlled directly – it does what it has been programmed to do. It is usually attached to another program and it requires a trigger to start its actions (e.g. starting attached program). The main feature of the virus is the ability to replicate, both in the infected computer and in the accessible network. Viruses can have different impacts on the infected system. The oldest known impact of security breaches is system slow down, because the virus uses all resources to replicate itself – using free memory and sending e-mails containing the virus to everyone. Or the virus may start deleting files, or completely blocking the system, thus preventing you from controlling it. Besides those visible effects, malicious code can also install special

[106] Anonymous, *Maximum Security: A Hacker's Guide to Protecting Your Computer Systems and Network,* (Sams: Indianapolis, 2002), page 46

programs that enable the creator to control your computer or monitor all your actions.

Worms are very similar to viruses, sometimes worms are regarded as a subclass of viruses. Their purpose is mainly to spread through the network, but they may have other tasks as well. The difference between worm and virus is that a worm is more independent – it does not require trigger to start its actions. It very often relies on unrepaired bugs and security flaws in operating systems or in other software.

According to the Symantec report,[107] the worst worm of all times is the Mydoom worm. This worm spread during 2 hours in January 2004 and caused damage worth of 38 billion USD.[108] The worm pretended to be an error message from the mail delivery system. When the recipient opened the attachment, worm sent emails to all addresses stored in the computer. So far it would behave more like a virus, but Mydoom also attempted to spread via peer-to-peer networks.

Another worm named Flame was discovered in 2012.[109] Its purpose was to gather information available in the computer and to get any information available, for instance capturing screenshots or pictures from the web camera. Gathered information was then transmitted. The Flame worm focused on the Middle East region. Its complexity and purpose suggests that it was designed for espionage purposes and was presumably state sponsored.[110]

Trojan horses can be regarded as a special kind of virus. It may be programmed to spread as well, but the main task of this software is to grant unauthorized access to the perpetrator

---

[107] Symantec Press Release, *Top 5 Viruses* (United Kingdom: Symantec, 2013), http://now.symassets.com/now/en/GB_SITE/pu/images/Promotions/2014/top-5-viruses/images/infographic_TOP_5_Viruses.jpg (accessed on 9th June 2014)
[108] Ibid
[109] Alexander Gostev, *The Flame: Questions and Answers*, (Russian Federation: Kaspersky lab, 2012), http://securelist.com/blog/incidents/34344/the-flame-questions-and-answers-51/ (accessed on 29th June 2013)
[110] Alexander Gostev, *The Flame: Questions and Answers*, (Russian Federation: Kaspersky lab, 2012), http://securelist.com/blog/incidents/34344/the-flame-questions-and-answers-51/ (accessed on 29th June 2013)

– so called back door. That is also the reason why this software appears to be useful to persuade the victim to download it. There are many ways of spreading Trojan horses. It may be hidden within freeware software, it may be distributed using fraud email messages with attachment or forgotten flash sticks.

Storm Trojan has been probably the most successful Trojan horse. It was released in 2007, it installed special a service and replicated to other computers. It also gained control over the computer, making it part of the botnet. In the meantime the service shared information with other computers in the botnet. It is estimated that in the highest peak the botnet consisted of more than 10 million computers.[111]

Botnets are networks of computers partially or totally controlled by a botmaster (sometimes called a zombie master). Computers may appear to work normally, but part of the computing capacity might be used by the botmaster for his own purposes. Originally botnets were created to gain large computing capacity that can be used to crack passwords. Nowadays they are used to generate immense amount of network traffic targeting a particular server or webpage (see below). Botnets can be obtained using Trojan horses or simply bought from the botmasters. Official botnets are used to analyze data from telescopes or for other research purposes. These botnets consist of users volunteering to share the capacity of their computers for the particular research purpose.

SQL[112] injection is a special technique exploiting the vulnerabilities of some data-driven application. Perpetrator inserts prepared SQL query to the badly secured interface with an error on purpose to gather information from the automated error log or he might be able to trick the system by some generic SQL command to get the data.

Ransomware is a term describing malware used to block the computer and prevent the

[111] Steve Bell, *Which is the worst computer virus in history? Here's our top 10,* (United Kingdom: BullGuard 2014), http://www.bullguard.com/blog/2014/03/which-is-the-worst-computer-virus-in-history-heres-our-top-10.html (accesses 6th June 2014)

[112] SQL stands for structured query language. SQL is a programming language used for working with databases.

owner from using infected device. The access might be encoded or blocked in a different way. The perpetrator demands a payment in exchange for unlocking the computer.

Spyware is a malware programmed to gather data about user's activity. It may be a keystroke logger or software designed to capture screenshots. The software would gather the information and then transfer it to the perpetrators.

Logical bombs are hidden commands in the code that will trigger in a specific moment. This moment might be a particular date and time in the future or a special set of conditions. The perpetrator in this case must be able to modify the original code, either during its creation or through fake update of the software.

8.4.2.2. Schemes

Schemes can be regarded as activities performed to achieve a given goal. The activity combines some of the tools mentioned above; for instance spamming with viruses. It is possible that in some cases the scheme is used alone depending on the goal of the perpetrator – e.g. spamming political ideas. There are described some of these fraudulent techniques to highlight the possibilities available to the perpetrators in cyber space. Of course that this list is not extensive and there are many special techniques combining more than one schemes with other tools as well.

Spamming in cyber space refers to the sending of unsolicited electronic messages in huge quantities. There might be a special rule how recipients are selected depending on the purpose of the spamming – if the aim is to promote particular product for men, apparently feminine email address should be excluded. But in many cases the recipients are random. The scheme of the spamming is simple – you receive an email you do not want to read. However, it might get your attention. Even if the impact is minimal, it is still worth the try since sending emails is virtually for free. On the other hand, spam creates significant costs to the recipients in total – it uses the computer space, capacity of email servers and the time recipients spend deleting the messages.

The danger of the spamming is based on the combination with social engineering or viruses. The spam message may not apply to be a marketing message, but a fraud message from a bank or a service provided. The more real the message looks, the higher probability that it gets through spam filters in the recipients computer. If the recipient is intrigued into opening the attachment or following a link, it may trigger an installation of a virus or a Trojan horse. Of course that the probability is in general very low, but increases with the numbers of recipients and therefore increases the probability of success – spamming one million emails costs around 10 USD.[113]

Phishing is a fraudulent technique attempting to get sensitive information. The victim usually receives an email appearing to be from a recipient's bank or a service provider. It might directly ask for some information (e.g. login information to user's account) or it might redirect the victim to forged web pages and lure them to enter demanded information; or to web pages infected with malware. In combination with spamming phishing can be very profitable cybercrime getting credit card information. The success rate is rather low as the phishing emails reach false targets (e.g. people who have never had an account with given company) or they are in foreign language or there are too many typos and errors.

However, the perpetrators started selecting their targets. This scheme is called **Spear phishing**. Spear phishing has the same target – getting sensitive information. But in this case the message is more personalized for every receiver. It may, for instance, contain the name of the recipient or list his recent activity.

Social engineering can be regarded as another level of spear phishing. Again the aim is to manipulate the recipient into performing particular action or providing desired information. For this purpose perpetrators do not use the spamming technique as they focus on several particular targets. The attack itself requires a preparation phase. Perpetrator collects information about the target during this period, for example from social networks or even spies on target's daily routines. The attacks do not have to be

[113] Ian Steadman, *Russian Underground Offers Cybercrime Services at Dirt-Cheap Prices,* (United Kingdom: Wired, 2012), http://www.wired.com/2012/11/russian-underground-economy/ (accessed 9th July 2014)

executed through email, but it may be done using a phone call. The perpetrator attempts to persuade the victim using a complex fraud scheme.

Blackmailing has the same characteristics in cyber space as in the real world. The perpetrator threatens the victim that he will damage or destroy his assets or even hardware using cyber attacks unless his demands are met. This scheme is often used by owners of large botnets capable of causing severe problems to the target. In such case it might be more efficient to meet perpetrator demands rather than to risk the collapse of the network or the outage of services provided to other clients. In some cases the perpetrator starts the attack and then presents his demands to stop his actions. This happened in the case of Feedly, RSS news aggregator. Its cloud based services were suffering from the DDoS attack and Feedly representatives were presented with the demand for payment to actually stop the attacks. The attackers were refused.[114] In other case, attackers gained unauthorized access to a customer database of Domino's Pizza in France and Belgium. Attackers demanded a ransom from the restaurant chain not to make the data public.[115]

Denial of Service attack (DoS) targets a webpage or a server and tries to generate critical volume of traffic so the target collapses. It used to be very difficult to distinguish this artificial traffic from legitimate traffic generated by everyday users. As a result, the service provided by the target was unavailable and thus the service was denied to legitimate users. However, the DoS attacks became less successful as the attacking botnets could be localized and thus the traffic from a particular nod or a country was rejected. The perpetrators than came up with the **Distributed Denial of Service attack (DDoS)**. The principle remains the same, but the artificial traffic appears to come from many different directions. It is therefore more complicated to separate the legitimate traffic and protect the target. This type of attack is using a brute force to bring down the target as there will always be a limit, after which the target will cease to provide the service.

---

[114] Graham Cluley, *Feedly refuses to give in to blackmail demands, gets hit by DDoS attack,* (United Kingdom: Cluley Associates Limited, 2014), http://grahamcluley.com/2014/06/feedly-blackmail-ddos/ (accessed 5th August 2014)

[115] Graham Cluley, *Internet firm goes out of business after DDoS exortion attack,* (Eset, 2014), http://www.welivesecurity.com/2014/06/21/internet-firm-ddos-extortion-attack/ (accessed 21st August)

Hacking refers to an activity of hackers, who attempts to find and exploit a weakness in the code, computer system or computer network. The community and differences among particular types of hacker will not be discussed; the focus will be mainly on their activity. Hackers got attention of the public attempting to gain access to well secured systems (e.g. FBI network) or braking (cracking) the code protecting some networks or devices (e.g. braking the manufacturer protection of mobile devices). Hackers attempt to find and exploit a weakness. The weakness might be in the code itself or it might be the concept of the code, or the usage of particular commands or even the architecture. It is simple to imagine an error in the code. Such error might disable a particular feature of the program, e.g. verification of user's authorization. If the hacker discovers this error, he might be able to modify some functionalities of the software and get access to the system. Errors that have not been discovered during the software development can be repaired by patches, which actually replace the wrong piece of code. Nevertheless, the weakness may not be an error in the code. It might be a simple usage of a command with particular characteristics that may be abused by the hackers. The chances that a hacker finds a weakness and knows how to exploit it are limited. However, then comes into the place the community. The community of hackers is very unclear and virtual, but still very efficient. Hackers are willing to share their experience and knowledge up to a certain extent. One hacker might find a flaw in the code. He spreads this information to the community and someone else will come with a way how to exploit this flaw. On the other hand, the level of cooperation among companies producing the software or among the cyber security companies is much lower, as they are direct competitors.

Bugs or exploitable errors can occur in code on purpose by programmers working on the code or simply by error. First of all let us focus on the second option. It is important to say that not every bug or error is exploitable and can be regarded as a security risk. Critical errors are only some of all the bugs and only a few can be exploited. The code usually goes through several test procedures and quality check controls that discover majority of issues or bugs. Especially critical problems influencing the main functionalities of the code are discovered very early in the process. The probability that critical exploitable error remains

in the software during all test rounds and is being actually in the distributed software is very low. Nevertheless, it grows with the complexity and the size of the code. The complexity of the code can be measured by the number of functional points, but this metric is not clearly defined and its interpretation might differ, as it is a qualitative metric. On the other hand the size of the code can be measured by the number of lines of the code (LoC). This metric simply counts the lines of the code used in the software. Since this metric is quantitative, the development is described in the following table:

Operation System Name	Release Date	Number of LoC (millions)
Windows 3.1	1992	2,5
Windows NT 3.1	1993	4,5
Windows NT 3.5	1994	7,5
Windows NT 3.51	1995	9,5
Windows NT 4.0	1996	11,5
Windows 2000	2000	29
Windows XP	2001	40
Windows Vista	2007	50

Table 5 – Number of LoC used in operating systems, based on data from Information is beautiful[116]

The table shows that number of LoC has increased in time. It is true that the number of LoC does not refer to the quality of the code, but it increases the probability of the critical exploitable error. The number of bugs and errors is sometimes referred to the number of LoC. Publications in 90s stated that from 10 to 50 errors can occur per 1000 lines of code.[117] Extremely well written code with focus on security is supposed to have one error per 1000 LoC.[118] Let us presume that Microsoft is such a company. Even then the Windows Vista would have 50 000 errors and bugs in the code. If the average in the U.S. is applied, 85% of these bugs and errors are discovered during tests.[119] Remaining 7500 bugs are in the

[116] Pearl Doughty-White, Miriam Quick, *Codebases,* (Informationisbeautiful, 2013), http://www.informationisbeautiful.net/visualizations/million-lines-of-code/ (accessed 18th July 2014)
[117] Vinnie Murdico, *Bugs per line of code,* (Tester's World, 2007), http://amartester.blogspot.cz/2007/04/bugs-per-lines-of-code.html (accessed 23rd June 2014)
[118] Chad Perrin, *The danger of complexity: More code, more bugs,* (United States: CBS Interactive, 2010), http://www.techrepublic.com/blog/it-security/the-danger-of-complexity-more-code-more-bugs/ (accessed 17th June 2014)
[119] Jim Bird, *Bugs and numbers: How many bugs do you have in your code?,* (Building Real Software, 2011), http://swreflections.blogspot.cz/2011/08/bugs-and-numbers-how-many-bugs-do-you.html (accessed 13th June 2014)

software and will be installed on users' computers. Approximately 1875 (25%) bugs are critical.

The second option is a sabotage. A programmer working in the development slips in the code an error or a piece of code designed to do harm or enable access into the system in the future. Ordinary bugs will not compromise the programmer, but a designed piece of code surely would. However, there are cases when programmers succeeded. In this example the aim was not to cause damage, but simply to make a joke (such pieces of code are called Easter eggs). In this case a programmer working on the Excel 97 included in the Excel code some other software – a flight simulator. Starting it required several steps, but it was possible. In some cases these Easter eggs are done on purpose and possibly even approved by the management to increase publicity. Special piece of code not relevant to the software purpose can be detected only by special test techniques or during peer review. It is difficult to estimate the probability of a programmer successfully sabotaging the code. However, since the length of the code is increasing, so is the probability. This influence might be related rather to the number of programmers working on the software than to the simple size of the code. In other words the larger the volume of the code needed, the larger is the number of programmers working on the software in order to launch the product according to the plan.

It is a common practice that developers from software companies analyze products of their competitors. During these activities they might come across various bugs or errors that were not discovered before the launch of the product. It is an unwritten rule that in such cases, the expert who discovered the flaw informs the producer of the software and publishes his results with a delay that allows the producer to release a security patch to remove the flaw from the software. In this way the possibility of the perpetrators exploiting this flaw is limited as they have to find the flaw first. After the announcement they can still come up with a way how to exploit the flaw, but they can target only computers or systems where the flaw has not been removed. Unfortunately, the time needed for the producer of the software to distribute the fix might take some time, up to several weeks. In 2013 a Google expert discovered an error in the Windows operation system that allowed the

perpetrator to gain same access rights as the current user of the computer. He reported his findings to Microsoft, but since he believed that Microsoft should act more quickly in similar cases, he announced that in one week he will publish his findings. Truly it took Microsoft more than one week to prepare and distribute security patch, it took almost two months. By the time the Google expert published his findings and Microsoft distributed the security patch hackers had managed to exploit this error in the system.[120]

8.4.3. Motivation of perpetrators

Cyber space offers many possibilities to perpetrators of all kinds. An incident occurred in cyber space, for instance famous online new website was brought down. This action caused financial damage to the owner of the website. To decide whether this was terrorist attack, cybercrime or activist protest, it is necessary to know the motivation of the attacker, because it might be any of these. If the motivation of the attacker was to black mail the owner of the webpage, it was a cybercrime act. If the attacker in parallel releases a message that he would bring down the webpage as a protest against its owner's cruelty to animals, it would be regarded as a hacktivism. If the aim of the attacker was to cause as much damage as possible, because his ultimate goal is to coerce a government, it would be considered as a terrorist act. The motivation of the perpetrator defines the goals of his actions and therefore influences his classification and the classification of his actions from the legal perspective. The motivation of the perpetrators can be divided into two major groups – political and personal. The political motivation is used in this analysis to describe the motivation related to the dissatisfaction of the individual (or group) with the current situation in the society he or she lives in or is associated with. Political motivation may lead the perpetrators to use tools mentioned above to perform acts of hacktivism or cyber terrorism. Personal motivation of the perpetrators refers to the desires of the individual. Perpetrators with personal motivation will possibly commit acts of cybercrime.

It is very difficult to define the exact motivation of the perpetrator and efficiently distinguish the border between the two main motivation types mentioned previously.

---

[120] Matouš Lázňovský, *Chybu zveřejněnou expertem Googlu využili hackeři před vydáním opravy,* (Czech Republic: Mafra, 2013), http://technet.idnes.cz/microsoft-oprava-chyby-0v1-/sw_internet.aspx?c=A130710_165204_sw_internet_mla (accessed 26th June 2014)

However, for the purpose of this analysis these two motivation factors will be considered disregarding any possible overlaps.

8.4.3.1. Cybercrime

Cybercrime is relatively a new phenomenon in the illegal activities. The motivation of the perpetrators is personal – perpetrator executes the action to gain personal benefits from the action, for instance to get money (e.g. advance fee fraud, credit card fraud) or to improve his or her status within the community (e.g. distribution of viruses).

The definition of cybercrime according to the Oxford dictionary is: "Criminal activities carried out by means of computers or the Internet."[121] Much simpler definition is that cybercrime is a criminal activity that requires usage of computer or cyber space and this usage is violating the law. The important fact is that any activity must be punishable by law to be labeled as a cybercrime.

The first criminal acts that can be today regarded as cybercrime would be telephone cards frauds, which appeared in late 80s.[122] Criminal activities in the virtual realm have been evolving together with the technology itself. Criminal acts committed on the internet are numerous and more and more sophisticated. As a result, total damages caused by cybercrime reached 113 billion USD globally.[123]

8.4.3.2. Hacktivism

Hacktivism is an activism in cyber space that uses some of the tools and schemes mentioned above. Activism itself is sometimes regarded as a criminal activity under certain legal conditions. The Oxford dictionary defines activism as "the policy or action of using vigorous campaigns to bring about political or social change."[124] Activists break the law during some of their actions and in these cases they can be prosecuted as criminals. Under particular

---

[121] Oxford Dictionary, http://www.oxforddictionaries.com/definition/english/cybercrime (accessed on 21st January 2013)
[122] Anonymous, Maximum Security - Hacker's Guide to Protecting Your Internet Site and Network, (Indianapolis: SAMS, 1998), page 37
[123] Norton, *Norton Cybercrime Report,* (United States: Symantec, 2011), http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/ (accessed 7th June 2013)
[124] Oxford Dictionary, http://www.oxforddictionaries.com/definition/english/activism (accessed on 21st January 2013)

conditions they may even be regarded as terrorists. For instance in 2009 FBI arrested four animal rights activists for possible criminal and terrorist activity.[125] The same applies to hactivism.

Hacktivism is per Oxford definition "gaining unauthorized access to computer files or networks to further social or political ends."[126] The term itself is connected both to known activist groups executing their actions in cyber space as well as in the real world and to new groups present only in cyber space. Greenpeace online activities can be given as an example for the first group of hacktivists. Greenpeace launched an online campaign against Nestlé as a protest against the usage of Indonesian palm oil during Kit Kat production in 2010. Indonesian rain forest was cleared to make way to palm plantations damaging the local habitat of protected animals like orangutans. The campaign used mainly social media and invited Internet users to post comments on Nestlé's Facebook profile. One million users saw Greenpeace Youtube advert on Kit Kat highlighting the damage done to orangutans. In the end Nestlé agreed to audit its suppliers and ensure more ecological resources[127]. The second group of hacktivists is represented by the group Anonymous or by the Wiki Leaks initiative. Whereas Wiki Leaks focus on data publishing, Anonymous is known to have a different approach. During a campaign called Operation Payback in 2010-2011, Anonymous members allegedly launched DDoS attacks against government facilities like Visa, Bank of America or the United States in reaction to closing of The Pirate Bay file-sharing website.[128]

8.4.3.3. Cyber terrorism

Cyber terrorism can be regarded as a usage of cyber attacks instead of more "conventional" physical attack with the same goal and motivation. For instance, instead of planting an

[125] Will Potter, *FBI Arrests 4 Activists as "Terrorists"for Chalking Slogans, Leafleting and Protesting,* (Green is the New Red, 2009), http://www.greenisthenewred.com/blog/aeta-arrests/1070/ (accessed 21st July 2014)
[126] Oxford Dictionary, http://www.oxforddictionaries.com/definition/english/hacktivist?q=hacktivism#hacktivist__6 (accessed on 21st January 2013)
[127] Martin Hickman, *Online protest drive Nestlé to environmentally friendly palm oil,* (United Kingdom: Independent, 2010), http://www.independent.co.uk/environment/green-living/online-protest-drives-nestl-to-environmentally-friendly-palm-oil-1976443.html (accessed 15th June 2014)
[128] John Ribeiro, *US charges 13 Anonymous members for DDoS attack,* (United States: PCWorld, 2013), http://www.pcworld.com/article/2052360/us-indicts-13-anonymous-members-for-ddos-attacks.html (accessed 8th July 2014)

explosive into a train terrorist may attempt to disable train control station causing derailment. Cyber terrorism is strongly dependent on the definition of terrorism as was discussed in previous chapter.

9. Cyber terrorism case studies

9.1. Introduction

Despite the fact that cyber terrorist attack has not been officially confirmed, many cyber attacks take place every day targeting governmental agencies, private companies and individuals. Nevertheless, the awareness of the possible consequences is rather low, as it is hard to imagine without relevant knowledge what can actually happen. One of the reasons is the fact that only minority of cyber attacks actually effected the physical world. But as this chapter will show, well aimed cyber attacks can have much more devastating effects that physical terrorist attacks.

The aim of this chapter is to compare the possibilities of cyber attacks with attacks committed in the physical world. Case studies are based on real events; wither from cyber space or from the real world. Alternative scenarios are created to actually evaluate both types of attacks.

9.2. Methodology

Simplified case studies method is used in this chapter to analyze the possibilities of cyber attacks compared to physical attacks from the perspective of terrorists. Simplified method is used because the purpose of this analysis is to demonstrate the possibilities of cyber attacks in general rather than to focus in deep technical detail on one particular case. Therefore the amount of collected data is limited in favor of the number of cases analyzed. The aim is to combine the qualitative approach of case studies method with deduction using more quantitative approach. Sixteen cases were selected as examples of both physical and cyber attacks in the sectors of critical infrastructure, financial sector and public sector. The cases were selected to demonstrate the possibilities in both dimensions. In some cases, the case only illustrates a particular feature that can be exploited in an attack. In such case both alternative scenarios have to be created to be analyzed afterwards.

For every case the alternative scenario is constructed using the existing examples or know schemes of attack to create an alternative to the original case in cyber space or in the real world. Both alternatives are then analyzed with focus on following criteria:

- Insider information
- Tools for attack
- Possible damage
- Physical presence
- Probability of success

The insider information criterion was selected because it is known to be crucial for the success of sophisticated cyber attacks. The attackers may use preprogrammed software or know security flaws, but additional configuration is needed to attack particular systems. The hypothesis is that cyber attacks will score significantly lower than physical alternatives.

Tools for the attack criterion describe the availability of tools required to perform the attack according to the scenario. This criterion partially includes needed financial or organizational resources to procure the tools. Intentionally soft skills or experience needed to perform the attack are excluded from this or from any other criterion. The reason is that this highly individual feature would be difficult to compare (e.g. skilled gunman vs. senior programmer).

Possible damage criterion reflects the damage inflected by the attack. It covers financial damage as well as possible casualties. This criterion is included because the inflicted damage is the basic goal of terrorist attacks. If the cyber attack alternative cannot inflict comparable damage, terrorist will not attempt to execute cyber terrorist attacks.

Physical presence criterion highlights the ultimate feature of the cyber attacks – attackers in general do not have to be physically present. The hypothesis is that cyber attacks will

score significantly higher in this criterion when compared to physical attacks. This criterion is included into the analysis presuming that the attacker wants to avoid being captured.

Probability of success criterion reflects the chances that the attacks will be successful and will inflict specified damage. This criterion is included in the analysis because the aim of terrorists is to successfully execute and attack to reach their goals. If the probability of success is very low, it may not be worth the effort even to attempt to execute such alternative.

Every criterion is awarded with points ranging from 0 to 10, 10 being the maximal amount of point, the higher the number of points the better. The range is used to better differentiate between physical and cyber attack alternative, but the amount of points cannot be used to express the general characteristics of the attack alternative. For example, 5 points for cyber attack probability of success criterion versus 1 point for physical attack alternative suggests that the cyber attack alternative is more probable to succeed, but the probability is still low. It does not mean that the probability of cyber attack alternative is 50%.

From sixteen presented cases, ten cases are analyzed in detail. These omitted cases are not analyzed either because of their resemblance to already analyzed case or because it would be difficult to analyze the case for the purpose of this chapter using described process.

9.3. Critical infrastructure

9.3.1. Bellingham Gasoline Pipeline, U.S.

9.3.1.1. Case

In 1999, pipeline Bellingham, U.S., ruptured and approximately 250 000 gallons of gasoline leaked into Hanna and Whatcom Creeks. The gasoline ignited and created a fireball that was travelling downstream killing persons, causing several injuries and significant property and environmental damage.

The investigation revealed that there were several reasons for the accident. Firstly, the place where the pipeline ruptured was physically damaged during terrain works in

previous years. This damage lowered the pressure capacity of the pipeline in this particular place. Secondly, the installed pressure relief valves were found to be improperly configured. Finally, during the accident the SCADA system operating the pipeline became unresponsive. The period of SCADA non-responsiveness collided with the moment of the rupture – when the pressure built up in the system, the operator was not able to start a second pump to lower the pressure.

The findings suggested that the SCADA problems might have been accidentally caused by administrators of the system performing actions influencing system's performance. Nevertheless, this hypothesis could not be confirmed due to the lack of evidence – needed logs were discarded during the emergency procedure run in order to restore the system.[129]

9.3.1.2. Comment

There was a chain of events in this case that resulted in the explosion. Despite the fact that the accident would not have happened without the physical damage done to the pipes or improper tests of pressure relief valves, it was the inaccessibility of SCADA terminal that made any possible attempts to prevent the explosion impossible. Given the fact that the system administrator left the control room for 15 minutes,[130] it might be concluded that his responsibility for the event is significant, therefore this accident might be classified as human error. Nevertheless, detailed analysis of this accident actually reveals that the responsiveness of the SCADA computer was influenced by the administrator preparing report based on historical data. Possible data queries regarding historical data might have actually influenced the SCADA system in a way that current data and operations were modified, the system slowed down and finally became irresponsive.

---

[129] Marshall Abrams, Joe Weiss, *Bellingham, Washington, Control System Cyber Security Case Study* (Mitre/NIST, 2007), http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Bellingham_Case_Study_report%2020Sep071.pdf (accessed on 27th November 2013)

[130] Ibid, page 12

9.3.1.3. Cyber attack alternative

Let us presume that the attacker would like to conduct a cyber attack on the basis of this case. This means that his target would be to overload the SCADA system and cause its failure or inaccessibility. This can be done using specially prepared malware, "self-destructive queries,"[131] initiate reboot of the system, delete critical data, etc. Given the fact that SCADA systems are usually backed up, it would be useless to put the system out of operation completely, as the backup system would take over. Moreover, such backups are usually placed in different location. The goal would be to influence the SCADA system in charge without triggering security mechanisms which would report a security incident and switch to backup system.

In order to prepare the "tool" for the attack (piece of code, virus, sql query, etc.), the attacker would need to have very specific information about the target system. He would need to know the type of the system, type of operations normally executed by the system, architecture of the system, nature of the data kept by the system and ideally security measures applied in the system. All these information can be obtained applying heuristic methods on other targets of similar nature – e.g. the attacker would try several attacks on different companies' SCADA systems to find out the typical response to certain action. The other way is to get these information from system documentation or other internal resources, but such information are usually classified and to gain access would mean to conduct separate cyber attack aimed at gaining such information (not impossible). Another option is to approach former employee or contractor who had access to such information, but the attacker would have firstly identify such person (again not impossible given all the information people publish online, like LinkedIn). The most sure but also most time demanding possibility for the attacker would to be to get hired to a position where he would have easier access to needed information or even to the system itself.

Once the attacker has all the information he needs, the preparation of the "tool" is the simplest part. He can use online resources or buy semi-finished malware.

[131] Queries that are written on purpose in a way that the system is overloading its capacities and possibly cannot display the result. Such queries might slow down the system of force reboot of the system.

The attack itself would require gaining access to the system, either directly or indirectly through any device like memory card. SCADA systems generally allow remote access, but the access rights might be limited. Gaining direct access to the system would require the attacker to physically get into the location where the terminal is placed and covertly use or install prepared "tool". The usage of a device would require infecting of placing the "tool" onto a device that is regularly in connection with the system network, e.g. administrator personal computer, memory card, smart phone, etc. Of course that there is security measures in place that should prevent such situation, but still the chances of success are high enough to at least try this option, especially given the fact that it is the simplest one.

9.3.1.4. Physical attack alternative

Possible attacker might prefer physical attack to achieve similar results as described in this case. Generally speaking, the alternative of physical attack resulting in the rupture of the pipeline followed by explosion exists.

Firstly, let's assume the option of physical damage done to the pipeline itself. The pipeline is not usually exposed in its entire length. When the pipeline is on the surface and it is accessible, it is logical to expect that security measures in place balance the probability of potential successful attack. In other words, successful attack on exposed pipeline might not have such destructive consequences as the described case. One of the reasons is also the fact that in case of exposed pipeline, there might be other sources of physical damage to the pipeline (e.g. extreme weather conditions). Moreover, the response would be immediate. The system would automatically start to stop the inflow of the product and alert security forces. Other option would be to choose remote location and use heavy machinery to get access to the pipeline and to create a rupture. In this case, the damage might be more serious, since it would be more difficult to make necessary repairs, but again the system would automatically minimize the consequences.

Second option is to attack critical nods in the pipeline network. Obviously, successful attack would have much more serious consequences, but also security measures in these places

would be much stricter and harder to overcome. It is also necessary to mention that such attack would require the knowledge of such place's location in the first place.

The procurement of necessary tools is another obstacle. The rupture can be done using heavy machinery. But such equipment is not suitable for stealthy and swift actions. Using explosives is an option, but again its provision is not as easy as it may seem. Homemade explosives in sufficient amount for such attack would require noticeable amount of ingredients whose purchase is monitored by security agencies. Gaining access to industrial or military explosives is not impossible, but it would be a significant obstacle.

9.3.1.5. Conclusion and points

Criteria	**Cyber Attack**	**Physical Attack**
Insider information	3	6
Tools for attack	8	2
Possible damage	6	6
Physical presence	7	1
Probability of success	3	8
Total	27	23

Both cyber and physical attacks alternatives on the basis of this case are possible. In both cases, the insider information is very important. In the case of cyber attack, it is the information about the SCADA system in place, system architecture and other ICT related information; while the physical attack requires information about geographical location. System related information is more difficult to obtain, because this type of information is created and kept internally by the company. Geographical information may be derived from maps or other publicly available sources. Despite the fact that the information needed for system malfunction are protected, it is more accessible when compare to information needed for system takeover.

Tools needed for the attack are no problem in case of cyber attack, but present a rather tricky obstacle for the physical attack as described above.

Possible damage caused by either physical or cyber attack would be similar. The main difference is that cyber attack is abusing the system and using it against itself, whereas the physical attack is more of external nature – the attacker must overcome physical security measures and then "fight" the system and its security procedures.

Physical attack requires the presence of the attacker in the place of attack. Cyber alternative does not require the presence of the attacker, but then the attack is not under direct control of the attacker. Physical presence is related to personal risk taken by the attacker.

The probability of success represents the control of the attacker over the attack itself. The number of points for cyber attack corresponds to the fact that in case of "remote" attack, there are too many possibilities that something will go wrong - the malware installs itself on a wrong computer thus revealing the danger of the device, protective software detects the dangerous content of the device and blocks the installation, target system refuses to execute the query, etc. On the other hand physical attack will be successful, but requires the "sacrifice" of the attacker – the probability of capture is rather high.

9.3.2. Maroochy Water Services, Australia

9.3.2.1. Case

Approximately 800 000 liters of raw sewage leaked from Maroochy Water Services into parks, rivers and private property as a direct consequence of cyber attacks aimed at SCADA system managing the radio-controlled sewage equipment of Maroochy Water Services in Australia.

The attacks were in reality forged instructions to particular water pump pretending to be sent from the system with enough authority to influence the function of the pump. In such way, the attacker managed to alter the data, intercept communication between the control center and particular pumps and cause other problems in the system resulting in the leakage of raw sewage.

The attacker in this case was a former employer of the company installing the control system in the facility. He sought to revenge this way for losing his job with the company. He used unique knowledge of the system he had to forge the messages and commands to the water pumps. These messages were transited on the same radio frequency the system used for communication.[132]

The attacker was sentenced in 2001. Sophisticated forensic activities were needed to prove that the attacker was responsible for the malfunctions of the system. It was also stated that there were no security defenses, neither any cyber security procedures.[133]

9.3.2.2. Comment

This case demonstrates the importance of insider information for successful cyber attack. The perpetrator revenged by causing malfunctions in the system he previously helped to build. The attacks resulted even in the overflow on one of the pump and in the leakage of raw sewerage. To execute the attack, he needed only ordinary computer and transmitter with needed settings. He then sent forged messages into the system and partially took control over certain segments of the system. It is not known if more serious damage was not caused due to the incapability of the attacker or thanks to his conscience. In this case the perpetrator was arrested in the end thanks to hard work of the system administrators and attacker's arrogance.

If the attacker shared his knowledge with determined terrorist, the consequences might have been catastrophic. This only highlights the fact that the number of people in possession of important information about critical infrastructure is rising. Moreover, external contractors are often overlooked as a potential source of security risk. Such people may not only be aware of systems' weak points, but also know about the system logic and therefore overcome possible security measures that would be taken right after the attack.

---

132 Marshall Abrams, Joe Weiss, *Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia,* (Mitre/NIST, 2008), http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf (accessed on 17th September 2013)

133 Tony Smith, *Hacker jailed for revenge sewage attacks,* (theregister.co.uk, 2001), http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/ (accessed on 17th September 2013)

It is virtually impossible to defend against such attacks. The reason is that even if the security risk is known to the management, for instance thanks to the penetration tests, the decision might be not to take any actions because of the low probability of successful attack and costs related to needed security measures.

9.3.2.3. Cyber attack alternative

Possible attacker trying to conduct attack on the basis of this case would firstly need the information about the system in place. He would need to find out that there is a dedicated analog radio system for the communication between central system and particular pumps. Afterwards, he would need to find out the frequency, on which is the transmission taking place and hack the possible encryption in place. In the end he would need to have the knowledge of communication pattern used in the communication, but this should not be so difficult once the attacker is able to capture the communication and decode it. To actually perform an attack, he would need to have the knowledge of the target system to forge such a message to create maximal damage. Given the level of knowledge, it might be sufficient to generate error message and trigger security procedures. But this would depend on the aim of the attacker.

The attacker might try to take control of the system, but in this case he only forged messages to cause malfunctions of the system and particular components.

9.3.2.4. Physical attack alternative

Physical attack alternative would require gaining access to the water cleaning facility, where pumps are located. In this case it would be more difficult, because water cleaning facilities have restricted access and the intruder would need to overcome physical security measures like fences.

If the aim of the attack would be to cause leakage of raw sewerage, the attacker would need either to manipulate the pump manually or destroy it in a way that the leakage is inevitable. Again, such action would probably require usage of explosives.

9.3.2.5. Conclusion and points

Criteria	Cyber Attack	Physical Attack
Insider information	2	8
Tools for attack	5	4
Possible damage	8	4
Physical presence	6	1
Probability of success	3	7
Total	24	24

The need of insider information for the cyber attack is crucial. Some information might be obtained on the spot by monitoring ongoing transmission, but again the knowledge of target system functionality and logic is necessary to create forged messages that would actually cause some damage. Specific software and installation setup was used in this case to actually make the transmission look like an authentic message. On the other hand physical attack requires only knowledge of the function of the facility in terms of where to execute the attack to cause maximal damage.

Cyber attack based on forged messages requires more detailed preparations of the messages. Suspicious messages in the system that would not resolve in the success of the attack would alarm the administrators that there is possible source of forged messages and it is very probable that they would take countermeasures to prevent any further forged messages getting into the system. In this case the attack must be successful rather swiftly before anyone notices the corrupted transmission and reacts. Physical attack alternative requires again usage of explosives, but it might be sufficient to manually interfere with the pump functionality.

If the cyber attacker manages to successfully forge messages, he is not in direct control of the system, but can try to make the system perform dangerous actions on a large scale. Of course, he might be limited by some security measures (e.g. system will not initiate complete stop of operations based on remotely received message without further authorization), but still the attacker can try to simultaneously influence more parts of the network. On the other hand physical attack can focus only on one place. Large scale attack

would be more demanding in terms of planning, preparation and needed resources. In this case the potential of individual attacker or small group of attackers is compared.

In this case the attacker would need to be in the receive radius of the target. This makes him vulnerable, but definitely less vulnerable than physical attacker who would need to overcome fence and other physical obstacles.

Once the cyber attacker has the information he needs and managed to prepare forged messages which will pass for the original transmission, the only security measures not discovered by previous research or swift reaction from the administrators and personnel can prevent the attack to be fully successful. The reason is that there is always an option to override the orders the pump received by manually disabling the device. Nevertheless, even if such action manages to successfully stop the attack in progress, the attack would manage to cause some damage in terms of financial loss. The consequences of the physical attack could not be minimized in the same way as in the case of cyber attack, because the devices that would be used tom manually override the received orders would be the targets of the attack. Therefore they would be either under the control of the attacker on destroyed. In the end, the probability of success of the attacker if he has all necessary information and required resources is higher than in the cyber attack scenario.

9.3.3. Davis – Besse nuclear plant, U.S.

9.3.3.1. Case

In 2003, traffic generated by infected computer system blocked the corporate and control network in the Davis-Besse nuclear power plant in Ohio. As a result, the safety parameter display showing sensitive data about reactor core was inaccessible for four hours and fifty minutes. This information is the first to indicate possible meltdown of the core or other critical problems in the reactor. However, in case of malfunction, the operators can access directly the analog readouts on the equipment.

Following investigation revealed that the traffic was generated by the Slammer worm. This worm does not carry any malicious payload, it simply generates traffic. The worm got into

the system through a computer of external consultant. Existing firewall protection in the power plant would have prevented the worm from infecting internal systems, but the consultant created a bypass to connect to his enterprise office. Therefore the worm avoided detection by the firewall and entered the corporate network first. Since there was no protection between the networks, it easily got also into the plant control network.

This incident did not cause any substantial damage. It only highlighted certain security risks that needed to be addressed. However, it also shows that very simple malware without being targeted or controlled can target even the nuclear plant.[134]

9.3.3.2. Comment

This incident appeared as a side effect of simple, yet destructive virus. The attacker did not target nuclear plant in particular, he simply released the virus on the Internet and let it spread according to is preprogrammed behavior. Surprisingly the dangerousness of the virus was not the deletion of file, loss of control or any such sophisticated functionality. It simply generated traffic. In some cases this traffic was high over the limits and it resulted in overflow and inaccessibility of the infected servers. From this point of view, it is similar to DoS and DDoS types of cyber attack (see above). Despite the fact that in case of this incident the problem was "only" not showing data in dedicated console, it demonstrated the risks related to the connection of critical infrastructure to the Internet. In this case, the nuclear facility was infected not because someone tried to find a way how to penetrate the security of the network, bud the virus simply used the security hole of one component used in the system. This transitive risk is a big security issue when OTS products are used in critical infrastructure because of price. Another example of this problem is the intended replacement of paper maps by iPads in the American Airforces,[135] as the reprinting is in the end more expensive then procurement of iPads. Of course, that it should be special

---

[134] Brent Kesler, *The Vulnerability of Nuclear Facilities to Cyber Attack; Strategic Insights: Spring 2010*, (Naval Postgraduate School: Monterey, 2011), pages 19-20, http://hdl.handle.net/10945/25465 (accessed on 15th July 2013)

[135] Rosťa Jančar, *Americké letectvo testuje pilotní mapy na vojenských iPadech mini,* (idnes.cz, 2013), http://technet.idnes.cz/letectvo-mapy-ipad-0n5-/notebooky.aspx?c=A130731_192627_tec_technika_rja (accessed on 21st September 2013)

military version of the iPad, but still there was no cyber security issue with the printed map, but with iPad there will be.

9.3.3.3. Cyber attack alternative

There was no particular target in this case and the incident was merely a result of a coincidence. For the purpose of this analysis, let us presume that the target is the inaccessibility of critical information in the system or planting false information into the system. This would be very difficult, because the attacker would need to know, what kind of system is used in the facility, how it works, what are the key servers, what is the type of the servers and much more information. The system itself would be probably industrial software customized for the particular facility. General knowledge obtainable online would be therefore limited and the attacker would need to gain access to the documentation describing the system. The same count for the servers and other hardware he might target. If the attack is supposed to be planned and under control the attacker must have information about the architecture of the system. He would need additional information to be able to plant false information into the system. Targeting the network infrastructure would be easier as the same happened in the case. But still the attacker would need to know, what kind of servers is used, what is the operational system etc.

9.3.3.4. Physical attack alternative

Physical alternative in this case would not make sense. It would require the attacker to gain access into the facility and actually damage some component so the numbers would be wrong. But in this case if the attacker is capable of penetrating the security, it does not make sense to undergo such risk only for this result. In this case he would probably try to stop the reaction in the reactor or to cause even more damage.

9.3.3.5. Conclusion and points

Criteria	Cyber Attack	Physical Attack
Insider information	2	0
Tools for attack	6	0
Possible damage	3	0
Physical presence	6	0
Probability of success	4	0
Total	21	0

For the cyber attack preparation insider information would be necessary. On the other hand the tools would be easy to prepare once needed information are available. In this case the possible damage is very low compared to the destructive potential of a nuclear plant. Not displaying correct numbers or even the shutdown of the systems responsible for providing such information would be a problem, but still easily solvable by checking the information from another source. The physical presence is not required, the infection spread over the Internet in this case. The attacker might not be successful with the same approach again, but he can still try to infect some device that will be connected to the network. The last resort would be to actually get physical access to some computer connected to the network. The probability of success is rather low due to the fact that the employees would have other ways how to verify the information displayed by the system.

9.3.4. Browns Ferry nuclear plant, U.S.

9.3.4.1. Case

In 2006, Unit 3 at the Browns Ferry nuclear power plant had to be manually shutdown as both reactor recirculation pumps and condensate demineralizer controller failed. Recirculation pumps are necessary for cooling down the reactor. As they were not functioning, the shutdown was needed to prevent the melting of reactor core and further problems.

All mentioned devices include microprocessors that communicate over local network – Ethernet. The investigation showed that in one moment, the control network begun to produce more traffic that the critical devices could handle under given configuration. This

resulted in the failure of devices critical for the security of the power plant. The traffic might have been caused by malfunction of one of the device or other component, but the findings of the analysis were inconclusive.

No intentional cyber attack or other external influence was found in this incident, but the analysis proved that such vulnerability could be exploited by very simple malware.[136]

9.3.4.2. Comment

No special attack or conditions were involved in this case. What is probably worse is the fact that no external interference was traced. Therefore it is not possible to clearly state what the reason of the high traffic that occurred in the network was. In case that also other network components were infected (e.g. by a worm like Slammer) and out of order, the results might have been much worse. Imagine if also sensors that would alert plant personnel were out of order.

For the purpose of this analysis let us presume that similar situation can be achieved also through cyber attack aimed at such critical components.

9.3.4.3. Cyber attack alternative

The attacker would need to know, what systems are used in the facility and what their capacity is. Important internal information is also the architecture of the network and interdependencies between particular components and the facility operations. Because if the ultimate aim of the attacker is uncontrollable reaction in the reactor, he would need to create the problem and also to suppress all warning systems.

Once knowing all details about the systems he is going to attack, the attacker would need to distribute the malicious software. Presumably, current security standards prohibit LAN in nuclear power plant from being connected directly to the Internet. The attacker may

[136] Brent Kesler, *The Vulnerability of Nuclear Facilities to Cyber Attack; Strategic Insights: Spring 2010*, (Naval Postgraduate School: Monterey, 2011), pages 20-21, http://hdl.handle.net/10945/25465 (accessed on 15th July 2013)

therefore rely on coincidental usage of infected device. For this he would need to identify devices with high probability of such connection (e.g. smart phones of employees, personal tablets). Another approach would be to intentionally "loose" some devices in places frequented by employers with access to the network. Of course that usage of such device in the power plant would be against basic security policies, but so called "road apples" can be still very effective way how to distribute malware.[137] He can also try to find security breach when someone violates the policy and establishes Internet connection from a device that is also connected to local network. Other option would be to gain direct access to a computer connected to the network.

9.3.4.4. Physical attack alternative

In this case the physical attack alternative is possible, but it would be extremely difficult. The attacker would need to get physical access to the facility, plan explosives on critical places to actually cause such problems that the nuclear reaction would become uncontrollable. Such action would involve procurement of explosives and other equipment to get through the security. The attacker would also need to know what the weak points are. Since the security standard is that nuclear power plant should endure plane crash, the physical destruction would not be easy.

9.3.4.5. Conclusion and points

Criteria	**Cyber Attack**	**Physical Attack**
Insider information	1	4
Tools for attack	7	2
Possible damage	9	9
Physical presence	5	1
Probability of success	2	5
Total	24	21

Insider information is again critical mainly for cyber attack, but neither physical attack alternative would be successful without such information.

[137] Bill Bunter, *How to Protect Against Social Engineering Attacks,* (Bright Hub, 2012), http://www.brighthub.com/computing/smb-security/articles/1313.aspx (accessed on 19th September 2013)

Once the cyber attacker has all needed information, the preparation of virus or other more suitable “tool” for the attack is rather easy compared to the physical attack alternative. The attacker would need equipment to overcome physical obstacles and also to get through security personnel present at the site. To execute the attack itself, he would probably need explosives in large quantities. This would require special resources and also some transportation. It is improbable that an individual would manage to conduct such attack. It would require well organized and specially trained group of attackers.

In both alternatives the possible damage is the same – uncontrolled nuclear reaction resulting in explosion.

The physical presence is ultimate for the physical attack. In case that cyber attacker does not find a way how to efficiently deploy the “tool” through Internet or other devices, he would need to get access to the facility and prepare a logical bomb that would be triggered later.

The probability of success is higher for the physical attack alternative. The reason is that the attackers would be able to proactively deal with any potential attempts of personnel to avoid the catastrophe. While in the cyber attack scenario the attack itself would not be under direct control of the attacker and the power plant personnel might try to manually stop the reaction. Of course that the attacker might try to establish direct connection from the facility network to the Internet or use existing one, but that would make it even harder for him in terms of needed internal information, physical access to the facility and it would also increase the probability of being detected.

9.3.5. Hatch nuclear plant, U.S.

9.3.5.1. Case

In 2008, Unit 2 of Hatch nuclear power plant automatically shutdown as the system evaluated the data it got from control system as critical – sudden drop in the water reservoirs of the reactor.

The data system got was actually influenced by a software update executed on a single computer. This update was official and dully scheduled. Nevertheless the consequence escaped the attention of responsible personnel. The computer collected diagnostic data form the process control network. The update was programmed to synchronize data on both networks. When the update took place, it reset data on the control network and thus triggered the shutdown.

No external influence was found in this incident. But it demonstrated that problematic architecture of the system or lack of experience with critical processes might cause significant problems to the critical processes in a power plant.[138]

9.3.5.2. Comment

This case is presented only to demonstrate possible problems related to the usage of ICT in critical infrastructure without proper knowledge of interdependencies and related risks. Possible scenarios and points would resemble to previous case and therefore this incident is not further analyzed.

9.3.6. Natanz nuclear facility, Iran

9.3.6.1. Case

In 2011 984 centrifuges at Iranian uranium enrichment facility were destroyed as they were rotating with higher speed than the critical level. This incident was not confirmed by Iranian side, but it is believed that it was caused by special malware called Stuxnet. Stuxnet is a worm presumably designed only for this purpose. It targeted specific components used

[138] Brent Kesler, *The Vulnerability of Nuclear Facilities to Cyber Attack; Strategic Insights: Spring 2010*, (Naval Postgraduate School: Monterey, 2011), pages 21, http://hdl.handle.net/10945/25465 (accessed on 15th July 2013)

in the Iranian facility manufactured by both local and foreign company. Stuxnet in the infected system faked data produced by the controllers monitoring the status of the centrifuges, in the same time it increased the speed of the centrifuges beyond the critical limit.

The Stuxnet attack against the Iranian nuclear program demonstrates the impact that a sophisticated adversary with a detailed knowledge of process control systems can have on critical infrastructures. It is also an example of malware causing physical damage to a component. The hypothesis that this attack was state sponsored and that Stuxnet was designed to target this particular facility is supported by several facts. First of all, Stuxnet infected various systems, but it is known to cause damage only in Natanz facility. Secondly, the complexity of the malware suggests that profound testing of the program was needed. Such testing requires special environment and knowledge of the target system. Moreover, the preciseness of the attack suggests that the attackers had very detailed intelligence about the facility, used systems and its weaknesses.[139]

9.3.6.2. Comment

The Stuxnet is one of the very few real life examples when piece of code was used to actually physically destroy something. It is true that there was no official confirmation from the Iranian side that it was the Stuxnet that actually caused the destruction of the centrifuges, but the link between the Stuxnet and the destruction is generally accepted. Even if this event demonstrated the possibilities of cyber attacks, it is imperative to emphasize the complexity of the Stuxnet. It was designed to attack one particular system customized in one particular facility. The level of insider information used in this case is enormous. The preparation required the knowledge of Siemens provided software customized probably by Iranian programmers in the facility. This case will not be analyzed further since it is similar concept as in the case of Browns Ferry. This case demonstrates the

[139] Brent Kesler, *The Vulnerability of Nuclear Facilities to Cyber Attack; Strategic Insights: Spring 2010*, (Naval Postgraduate School: Monterey, 2011), pages 21, http://hdl.handle.net/10945/25465 (accessed on 15th July 2013), pages 21-22

importance of insider information needed for attacks that are designed to precisely attack one particular target.

9.3.7. Oak Ridge, Tennessee

In 2012, security forces arrested three demonstrators hosting banners and spraying messages on the walls. This incident took place in the Y-12 National Security Complex, supposedly one of the most secure places where enriched uranium and other resources potentially usable for nuclear weapons were stored.

The demonstrators were not armed and even did not carefully plan their action. One sister aged 83, and two other activists aged 57 and 63 equipped with lights and bolt cutter walked through security fences without any problems and without any response from the security forces. Finally, they reached the facility buildings and started to hoist banners. Their adventure took several hours, when they freely moved across one of the supposedly most secure nuclear facilities.

They were arrested and charged for trespassing and injuring national-defense premises in the end. However, this incident pointed out that the common opinion that such facilities are well protected and practically impenetrable might be wrong.[140]

9.3.7.1. Comment

The facility whose security measures were breached by activists is not a nuclear plant. However, it is a highly protected area on comparable level with nuclear power plant. In previous cases one of the major setbacks related to physical attack alternatives was the physical presence and physical security measures. This case illustrated that even in the most restricted places the security measures might not be as strict as they appear. It is true that the three activists were not a real threat, but had the same conditions been in place when determined terrorists properly armed and equipped got into the facility, the

[140] Tricia Escobedo, *Nun, two others in federal court for nuclear breach,* (CNN.com, 2013), http://edition.cnn.com/2013/05/07/justice/nun-nuclear-breach-charges/ (accessed on 21st September 2013)

consequences would surely be much more serious. Nevertheless, this case will not be further analyzed as its sole purpose is to demonstrate that physical attack may not be as difficult as it seems.

9.4. Financial sector

9.4.1. South Korea cyber attacks

9.4.1.1. Case

In 2013, the logic bomb triggered deletion of hard drives of infected computers across the South Korea. The attack targeted broadcasting companies KBS, MBC and YTN as well as financial sector; namely banks Jeju, Nonghyup and Shinhan. In result, the networks of all targeted companies were paralyzed; ATMs and smartphone banking websites were disabled. All companies were able to restore their operations till the next day, but the loss of data caused significant financial damage, not mentioning the damage to the trust of customers.

The attack itself started presumably on 19th of March, when spam messages appeared. These messages seemed to be coming from a bank. Attached file worked as a downloader for files containing malicious software. The software was programmed to trigger at a precise moment (therefore classifies as a logic bomb). The main task of the malware was to delete data from the infected computer, overwrite the hard drive and reboot the system. In the same time, the malware also searched for Linux machines connected to the same network as the computer. There was a module in the malware searching for remote connections using stored credentials to access Linux servers in order to delete their master boot record.

Attacks that started in March continued till June 2013 and according to the South Korean politicians were perpetrated by North Korea or related hacker groups. Total damage caused by these attacks was calculated to reach 470m GBP. [141]

[141] Alex Hern, *North Korean 'cyberwarfare'said to have cost South Korea £500m,* (theguardian.com, 2013), http://www.theguardian.com/world/2013/oct/16/north-korean-cyber-warfare-south-korea (accessed on 20th October 2013)

9.4.1.2. Comment

It is difficult to say what the aim of the attack was, as the identity of the attackers have not been verified. There was a defacement performed by a group called WhoIs Team claiming that they were the authors of the virus, but the authenticity is doubted. This attack had verified impact on TV broadcasting and financial institutions, but it is possible that the number of affected subjects was even larger. Material damage was quantified to reach 470m GBP,[142] but this amount is related to attacks that occurred during the whole period from March till June 2013. The damage caused by the attack describe in this case was at least 150m GBP, when considering stated facts. But probably the most serious damage was done to the trust of people in the financial system and its security.

For further analyses let us presume that the goal was to disable online banking.

9.4.1.3. Cyber attack alternative

The attacker attacked anyone who clicked on the link in the spam message. This resulted in the installation of the virus and later in the unavailability of service. The attackers trying to reach the same result might choose either similar way as described in the case, or use strength to bring down critical serves.

The first option is more sophisticated. Attackers need to know, what the target system is. They will also have to find a way how to get the virus into the system. In the described case the attacker used phishing. This method is very ineffective, but just few initially infected computers might be enough to cause serious problem, even the disruption of services.

The second option does not require any knowledge of used systems. DoS or DDoS type of attack simply rely on brutal force that takes down servers operating the target gateway. Attackers can prepare or buy botnets online and use them for the attack. Practically any server can be brought down by DDoS attack; it is just the matter of used resources. The

[142] Alex Hern, *North Korean 'cyberwarfare'said to have cost South Korea £500m,* (theguardian.com, 2013), http://www.theguardian.com/world/2013/oct/16/north-korean-cyber-warfare-south-korea (accessed on 20th October 2013)

attack scenario is simple – botnets generate requests that flood the target, in our case webpage hosting the gateway to online banking. When the number of requests reaches critical level, the server is not able to respond and the service becomes unavailable. Of course that there are several security measures that can deal with such attacks, but only up to a certain point. The critical problem of the protection against DDoS attacks is to determine which requests are illegal and artificially generated and which are legal and should be processed. When there are only several sources generating the illegal traffic, it is possible to redirect the traffic from these sources. Of course, more efficient is to cooperate with local ISP and shut down the servers generating this traffic, but this approach is sometimes not possible due to affiliation problem and lack of international cooperation. DDoS attack is still under control of the attacker, so they can react to any attempts to defend the target. Important features of the attack are the amount of traffic generated and the diversification of source servers across the internet. If the attack is well planned and well performed, the success is almost sure. The question is how long the attacker can keep the target out, because the administrators may relocate the gateway to different server, gather available capacities and prepare their position to defend against the attack.

9.4.1.4. Physical attack alternative

If the goal is to bring down online banking system of a particular bank, the target of the physical attack alternative has to be the infrastructure running the system. The target may be very specific – particular server, optical cables connecting the server to cyber space, electric cables powering the facility where target server is located, there are many ways how to impact cyber space attacking a physical target. However, it is necessary to have information about the target and its architecture. The attacker must know where exactly is the target located. In the scenario when the target is only a way how to reach main objective (e.g. disrupting optic cables), the attacker must be sure that such attack will really have desired impact and that there is no backup solution that would minimize the impact of the attack.

Apart from the insider information needed for the attack, attackers will need tools to execute such attack. In this case explosives or weapons might be needed. One of the

problem attacker will face is the physical location. Such important infrastructure will surely have its backup. While the cyber attack does not need to consider the physical location of the target, because the attack will gradually destroy or disable primary system and afterwards the backup. The fact that backup servers might be located in different state makes it harder for the attacker to execute the strike in an effective way. Despite the fact that the relation between cyber space and physical infrastructure is often ignored, many companies protect such systems not only from natural disasters but also from potential physical attacks. Nevertheless, such protection should be weaker when compared to nuclear facilities and to other critical infrastructure objects.

9.4.1.5. Conclusion and points

Criteria	**Cyber Attack**	**Physical Attack**
Insider information	8	3
Tools for attack	8	8
Possible damage	9	6
Physical presence	9	3
Probability of success	6	3
Total	40	23

Regarding insider information, the situation will be easier for the cyber attacker. He does ultimately need only the webpage where the gateway to online banking is hosted. Whereas the physical attacker need to find out the location of his target and also the logic relation among particular components to execute the attack in such a way that it has desired impact.

Given the fact that physical attacker can execute the attack with basic tools, both alternatives receive the same number of points. The reason is that also cyber attacker can easily procure needed tools, in this case presumably botnets capable of generating desired traffic. Since the botnets can be bought over internet, he does not have to create them on his own using Trojans and other malware.

Cyber attack alternative can cause much more damage as the target itself is also located in cyber space. Physical attack can damage the components needed to offer the service, but the administrators might find a way how to replace the attacked hardware or they can find an

alternative solution. Whereas in the cyber attack variant they have to repel the attacker first and restore the services afterwards.

Despite the fact that important infrastructure from this case might be less protected than national critical infrastructure, the physical presence required in the physical attack scenario creates risk that is not present in the cyber attack alternative.

The probability of success is higher in the case of cyber attack. The reason is that in the physical attack alternative, the administrators might respond to the attack in a better way as business continuity plans and procedures count with the possibility of a natural disaster damaging part of the needed infrastructure. Of course that in the case of well-planned attack, the consequence can be more serious than in case of fire or flood, but still the system itself is intact. It is only problem of the hardware. But in the case of the cyber attack, it is the system itself that is in trouble. The capacity of the hardware is not sufficient and the system is not able to operate. Replacing the hardware or redirecting the traffic might work for a while, but it does not prevent the attacker from launching another attack or simply redirecting that attack to a different webpage.

9.4.2. Disinformation and its impact on financial markets, U.S.

9.4.2.1. Case

In 2013 Dow Jones Industrial Average on the American stock market experienced a drop about 150 points – from 14697.15 to 14548.58. This decrease was caused by the message on Twitter account of the Associated Press: "Breaking: Two Explosions in the White House and Barack Obama is injured." The decrease started at 1:07 PM. The decrease ceased at 1:10 PM when the new that the message was forged begun to spread. The index returned to 14690 by 1:13 PM.

It was discovered later that the Twitter account was hacked by the attackers using phishing to get needed credentials for access. Despite the fact that the influence on the market was very short, it erased 136 billion USD in equity market value.[143]

[143] Max Fisher, *Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?,* (washingtonpost.com, 2013), http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/syrian-

9.4.2.2. Comment

In this case the attacker chose not to attack the main target itself, but rather to influence public opinion and spread false news in order to create panic and cause economic damage. The New York Stock Exchange was not the target. It would be difficult to prove that the real intention of the attackers was to destabilize the stock market. The false message was of such nature that it would have affected much more subjects, not only in the financial industry. The key factor in this case was the time that it took to produce and distribute the denial of the false message and the confirmation that in reality nothing had happened. It took only three minutes to deny the authenticity of the message, but still it was enough to cause fall in the Dow Jones index value. If it took longer, the attack might have started to have impact on banks and other industries as well. But thanks to rapid reaction it influenced only the stock exchange.

The real reason that enabled success of this attack is the approach of public to information and also the way contemporary journalists work. Nevertheless, none of these factors is the subject of this analysis.

Potential danger exploitable by terrorists or other attackers is that Twitter accounts or newspaper web pages are not regarded as critical infrastructure. The protection of such web pages or related servers is based on enterprise standards and it is up to the management to decide what level of protection the company can afford to finance. On the other hand information published online is one of the main sources of information for the public. This theory is supported also by the decrease in sales of printed newspapers and magazines. In some cases online news often quote other sources to inform the public practically in the real time. The competitiveness and drive to publish the information as soon as possible make it very difficult to verify the information before it is made public. Therefore if the attacker targets multiple news portals simultaneously, the disinformation

---

hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/ (accessed on 28th September 2013)

would start to spread faster and it would take public authorities much more time to persuade the public that the message was false and to mitigate the impacts.

Another important factor is the time. For how long would the main news portals have to display a message that one particular bank is in troubles and soon will ban withdrawals before a run on the bank starts? To defend against such attack, it is imperative to communicate the real state as soon as possible.

9.4.2.3. Cyber attack alternative

Cyber attack scenario is described in the case. However, to have a real impact on the economy and to be more of a terroristic attack, the perpetrators would have to simultaneously attack several targets at once. The best way would be to gain control of the online news portals to block any attempts to deny or remove the false message. In the case the attackers simply inserted the message in one information source and the reaction took only couple of minutes. Such action might be sufficient for a crime (e.g. false information about a company to buy shares at better price), but to cause serious economic damage the attackers would need more sophisticated tools.

To gain control or let's say administration rights to post content and block all other users the attacker will need to infect target system with Trojans. This can be done using phishing emails, spreading specially designed viruses or using social engineering. The probability of success might be above 50% for one target, but the necessity of posting the false message on several main news portals reduces the probability. The process itself would be more difficult for online newspapers then for Twitter or similar channels, as the message would have to be in form of article with certain format and wording to make it plausible.

Despite the fact that large scale attacks are not so easy to execute and the probability of success is rather low, even small scale attacks can disrupt the trust of the public and potentially cause some economic damage.

9.4.2.4. Physical attack alternative

It is not an alternative to fake the message in the printed newspapers as the number of readers is decreasing and it would be very difficult to control such attack. The attacker would need to physically force the people with needed access rights to post the intended message. This alternative is not impossible, but very difficult to execute in a large scale. The attacker would have to be well organized and know who exactly in every company running the new portals have necessary access rights. Once discovered that the messages are false, administrators would deny the access to the users "under control" of the attackers. The question is whether it would make sense for the attackers to use so many resources on such kind of action with unsure results.

9.4.2.5. Conclusion and points

Criteria	**Cyber Attack**	**Physical Attack**
Insider information	6	5
Tools for attack	5	6
Possible damage	8	6
Physical presence	9	1
Probability of success	4	2
Total	32	20

Insider information is needed mainly for the physical attack, if the cyber attack alternative is focused only on forging messages. If the aim is to take over the control of target systems, the need of internal information is higher.

Tools needed for both alternatives can be easily procured if the physical attackers follow the plan to hijack or force particular users to post the content. Even the most complex software needed for the attack can be procured from the Internet and customized afterwards. Nevertheless, the physical attack alternative cannot be done by one individual.

Possible damage depends on the intended goal of the attack. The goal is not the disruption of the trust to the particular news portal, but to spread panic and cause economic damage. If the attackers manage to block attempts to deny the forged message on targeted portals, the damage will increase with every minute.

Physical presence is not required for the cyber attack alternative, while it is necessary for the physical attack.

The probability of success is determined by the ultimate goal of the attack, for instance, to provoke a run on a bank. The probability to incite such reaction is rather low given the number of factors included in the scenario. Even if the attackers succeed in posting faked message and in blocking any attempts to remove the content, it is difficult to presume the reaction of the public.

9.4.3. JPMorgan card data loss

9.4.3.1. Case

In July 2013, JPMorgan Chase & Co issued a warning to 465 000 holders of prepaid cash cards that their personal information might have been acquired by hackers. These hackers penetrated the network and despite the fact that personal data of the customers is kept encrypted, the data were readable to the hackers as the encryption was not applied for this particular file format. The bank believed that only a small amount of data was taken and definitely not critical personal information as birth dates or social security numbers. [144]

9.4.3.2. Comment

This case is described as a criminal act. The attackers planned to acquire information needed to steal money from personal accounts of card holders whose data had been stolen. This type of attack would have to be executed on larger scale with the purpose of disrupting the trust in the banking system so it could be regarded as an act of terrorism. More problems could be caused by adding money to personal accounts and encouraging people to spend them, rather than stealing their money. But changing the account balance is more difficult than to steal money from the account using credit card or personal information.

---

[144] David Henry, Jim Finkle, *JPMorgan warns 465.000 card users on data loss after cyber attack,* (reuters.com, 2013), http://www.reuters.com/article/2013/12/05/us-jpmorgan-dataexposed-idUSBRE9B405R20131205 (accessed on 5th January 2014)

Setting account balance of individual customers to zero will be considered as the attacker's goal for the purpose of this scenario. The number of affected customers must be high enough to create substantial economic damage and also to damage the trust in the banking systems. Let us presume that the target number is similar to the case – 450 000 customers.

9.4.3.3. Cyber attack alternative

The first step in the cyber attack alternative is to acquire needed information to actually steal the money from the credit card accounts. Let us presume that the preferred way would be to use the credit card information to make false payments and thus reduce the account balance. Needed information can be obtained either from the system or database by stealing the data from the service provider, or using installed devices in the ATMs, sending phishing emails, establishing false payment gateways or using more sophisticated other tools (see next case for an example). There are many ways how to get needed information, but it is necessary to admit that they are very time consuming and the result is unsure. The most efficient way is stealing the data from a database, but this is also the most difficult option.

Once all needed information is available, the attacker can proceed with creating transactions for stealing the money. The problem might be transaction limits and other security measures. For instance, the owner of the card might have a constraint on the maximal amount available for online transaction per week. When such limits are exceeded, the bank should refuse to execute such transaction. Obviously, if the occurrence of such transactions with similar pattern starts to appear, the bank will notice and will follow its security procedures. The attackers would have to override such limitations, but that should be impossible without access into the system. Another option would be to gradually steal small amounts, but the probability that the owners will notice is high. Such action would be also very time consuming.

Therefore the number of acquired credit card information would have to be significantly higher that the target number of affected customers, as security measures and limits would protect some customers from one time false transaction account wipeout.

9.4.3.4. Physical attack alternative

Physical attack alternative is actually impossible. It would not be sufficient to rob the bank. In such case, the money would disappear from bank's account. Customer accounts would be influenced by bank's liquidity problems, but their account balance would be the same. The attackers would have to rob every one customer from the target number – 450 000 affected customers. Physical attack alternative cannot simultaneously impact the same number of targets as in the cyber attack alternative.

9.4.3.5. Conclusion and points

Criteria	**Cyber Attack**	**Physical Attack**
Insider information	6	0
Tools for attack	4	0
Possible damage	3	0
Physical presence	5	0
Probability of success	2	0
Total	20	0

No insider information is needed for this type of cyber attack. In this case insider information refers to internal bank data. Information needed for the attack itself as credit card number, will be obtained during first stage of attack using phishing email or other tools.

Attacker needs two types of tools – firstly tools for collecting needed information, secondly tools for generating payment transactions to actually steal the money. There are many options for both categories. The amount of points for this criterion reflects the size of the target group. The tools themselves can be easily obtained, but the efficiency is very low, or the procurement is very difficult (e.g. hacked terminals), but their efficiency is high.

Possible damage is short term. Banks have all data backed up. When the attack is discovered and explained, original balances should be easily restored. Therefore the damage would occur only till the attack is identified and explanation is accepted by banks and other financial institutions. Despite the fact that in the end attacked customers should not suffer from the financial loss, the attack will impact them for couple of days. Careful

timing of the attack may increase the caused damage (e.g. before Christmas), but it will be only temporary.

Physical presence of the attacker is not needed in general, but usage of certain tools may require physical presence in the first phase when collecting necessary information.

Given the fact that similar attacks have already occurred in smaller scale, the probability of success on big scale is very low. The probability is also influenced by security measures like maximal transaction amount.

9.4.4. Card terminals fraud

In 2008, European law-enforcement forces discovered a highly sophisticated credit-card fraud scheme. The criminals in this case used special device inserted in credit-card readers manufactured in China. The devices send account data to computer servers in Pakistan. This data have been used to make bank withdrawals and online purchases in several countries. The estimates are that so far the losses range of 50 million to 100 million USD. There is no way how to visually identify hacked device. However, investigators discovered that altered machine is slightly heavier than the standard credit-card reader. Using this information investigators were able to find the devices in at least five countries: Britain, Ireland, Belgium, the Netherlands and Denmark. They have been used in grocery chains including Asda, which is owned by Wal-Mart; Tesco; and Sainsbury.[145]

9.4.4.1. Comment

This is a very complicated criminal scheme that involved manipulation of many credit card terminals. It was not proved if the manipulation took place in the production factory, later during the shipping or just before the installation. Nevertheless, used microchips had to be prepared in advance in large quantity. The criminals in this case had to be sure that they will be able to control the device remotely and more importantly to use gained data to steal money. The case will not be further analyzed because of lack of information and also due to

[145] Siobhan Gorman, *Fraud Ring Funnels Data From Cards to Pakistan,*(wallstreetjournal.com, 2008), http://online.wsj.com/news/articles/SB122366999999723871 (accessed on 21st September 2013)

its complexity. However, it is very important example of potential security risk related to procurement of hardware.

The risk of using finished or semi-finished components in financial or telecommunication systems, military networks or critical infrastructure is similar to this case. Given the large number of hardware used in the systems and networks makes it very difficult to execute detailed control if the procured component does not contain special chip or software which may be later used in cyber attack or for criminal purposes. The actuality of this risk is highlighted in the report of House Intelligence Committee,[146] claiming that Chinese technological companies and potential cooperation with them might lead to security risks. This aspect is also discussed in the book Cyber War,[147] where author claims that majority of computers and other hardware in critical infrastructure came from China and therefore China has far better position in potential cyber conflict when compared to the U.S.

9.5. Public sector

9.5.1. London underground bombing

9.5.1.1. Case

In July 2005, explosions in the London underground and in a bus paralyzed London. The attackers detonated the explosives simultaneously in three trains going from King's Cross station. One hour later the last bomb exploded in a crowded bus. 39 people were killed in the underground transit system, 13 people died in the bus. More than 700 people were injured during this attack. In result, the whole underground transit system was closed for investigations.[148]

---

146 The Associated Press, *China tech firms pose security risk, U.S. panel warns,* (cbcnews.ca, 2012), http://www.cbc.ca/news/business/china-tech-firms-pose-security-risk-u-s-panel-warns-1.1286366 (accessed on 21st October 2013)

147 Richard A. Clarke a Robert K. Knake, *Cyber War,* (HarperCollins: New York, 2010), page 62

148 Michael Ray, *London bombings of 2005,* (Britannica.com, 2013), http://www.britannica.com/EBchecked/topic/1696348/London-bombings-of-2005 (accessed on 15th October 2013)

9.5.1.2. Comment

Despite the fact that the attacks were well planned and the execution did not fail, the number of casualties might have been much higher given the number of people using the London underground system every day. Right after the attacks, further consequences of the terrorist attacks appeared. People were afraid to use public transportation, increased police presence in the streets, closed underground because of ongoing investigation, all these factors were increasing the fear among public, which was the main goal of the terrorists.

9.5.1.3. Cyber attack alternative

Let us presume that the target is to cause explosions in the underground system, to enable analysis of the cyber attack alternative. The reason is that there are practically no explosives in the underground system that the attacker might try to use. Even if there were some explosive components, it is not very probable that they would be connected to the internal network or even to the Internet. In the cyber attack alternative, the attacker might try to cut off the supply of electric energy to stop the trains. Of course that if successful, such attack would cause substantial economic damage depending on how long the blackout would last. But there would be neither explosion nor casualties. The attacker might try to corrupt the traffic control system or gain control of that system to actually cause collisions or derail.

It is much more difficult to gain control of the traffic control system than to disrupt its functionality. If the attacker wants to disrupt the system, he might target particular components or communication bottlenecks exploiting weaknesses in the components or used software. Attackers might use “ordinary” viruses to overflow servers’ capacity or to disrupt the communication. The traffic control system itself would be specialized software. To gain control of such system, attackers would have to have very deep knowledge of the system in general and also of the system architecture used in the target system to avoid security measures implemented in the system. For both alternatives, the attacker will need insider information.

Given the importance of such system as underground traffic control system, the security measures should be adequate. Direct connection from the Internet should be impossible. The attacker aiming at disrupting the functionality of the system might use phishing, road apples, social engineering and other techniques to actually get the malware to the target system. Once there, the malware will commence the attack based on its software and further control is not necessary. If the attacker wants to gain the control of the system, he needs to get connected to the system. This might require his physical presence in the facility to actually gain the connection, if other attempts to connect via Internet fail.

9.5.1.4. Physical attack alternative

Physical attack alternative would resemble very much to this case. Considering the fact that the attacks took place in London, newly introduced security measures created more obstacles for the attackers to repeat such attacks. But still if carefully planned, the attackers might succeed.

9.5.1.5. Conclusion and points

Criteria	**Cyber Attack**	**Physical Attack**
Insider information	3	9
Tools for attack	6	3
Possible damage	8	7
Physical presence§	4	0
Probability of success	2	7
Total	23	26

Insider information is needed only for the cyber attack alternative. Physical attackers do not need to know anything about internal systems. The might be interested in knowing physical security measures in place, but they may proceed with the attack without such knowledge. Despite the fact that the knowledge of information needed for cyber attack alternative is more spread nowadays than in the past, the procurement of such information would be still very difficult.

Tools for the attack can be easily obtained for the cyber attack alternative, especially in the case that attackers would try to exploit weaknesses in particular components, not in the

system itself. Introduced security measures are supposed to make it more difficult to get access to explosives or to materials that can be used to make explosives. However, the number of substances usable for such purpose is still high. Of course, it would take long time to get enough resources to produce large quantity of explosives unnoticed. In the end, it is still possible to make explosives from available resources and keep low profile.

Physical attack damage will depend on the number of attackers, used amount of explosives and on other factors. But in the end, the system itself is prepared to minimize the inflicted damage. The attackers might destroy several wagons or even trains depending on their numbers. Buy if the cyber attacker gains control over the system, he might try to damage all trains at once.

Physical presence is essential for the physical attack alternative, especially if the attackers are suicide bombers; whereas for the cyber attack alternative, this factor is necessary only if there is no other possibility to establish connection with the target system or component.

Despite introduce security measures, the probability of success is higher in case of physical attack scenario. X rays in the underground systems are introduced only somewhere and it is not possible to check every passenger. The probability that a cyber attack would disrupt the system through targeting one particular component is higher than the probability of taking over the whole system, but still it is relatively low.

9.5.2. 9/11 attacks

9.5.2.1. Case

In September 2001, 19 militants from al-Qaeda hijacked four planes and committed the deadliest terrorist attacks on American soil in the U.S. history. Terrorist used hijacked planes as weapons and crashed them into their targets. Two planes crashed into Twin Towers Center in New York, one plane crashed into Pentagon and the remaining plane crashed in Pennsylvania when passengers attempted to retake the control of the plane.

Some 2750 people were killed in New York, 184 at the Pentagon, and 40 in Pennsylvania. More than 400 police officers and firefighters died during rescue works in New York.[149]

9.5.2.2. Comment

Worst committed terrorist attacks on the soil of the U.S. that have been committed so far started the global war on terror. 9/11 attacks also triggered introduction of new security measures and also became a worldwide known synonym of a terrorist attack. Despite the fact that it was not the first usage of a civil plane as a weapon, the scale and consequences surprised even famous experts on terrorism.

9.5.2.3. Cyber attack alternative

Cyber attack alternative would have to focus on different targets. In this case, terrorists took over the planes and used them as weapons to cause destruction. Cyber attacker cannot take control over the plane. Despite the fact that modern planes are full of computers and other modern technologies, the control is still in the hand of pilots. However, theoretically it is possible for the attacker to attack the systems used in planes and made it much more difficult for the pilots to actually control the plane. The situation would be different in the case of unmanned aerial vehicles like drones (see case below).

One of the options might be to actually plant special device or software into the hardware of the plane computers and use them later as a logic bomb or Trojan horse to gain remote access into the system. This can take place during manufacturing process or maintenance. Such scenario is theoretically possible, but it has very low probability of success given the strict control during manufacturing. It would be also extremely demanding in regard to needed financial and other resources.

In order to cause maximum damage, attacker may focus on ground targets – air traffic control systems. These systems belong to national critical infrastructure and should be well

[149] Peter L. Bergen, *September 11 attacks,* (Britannica.com, 2014), http://www.britannica.com/EBchecked/topic/762320/September-11-attacks (accessed on 18th February 2014)

protected. Nevertheless, the attackers may still try executing the attacks. In a study published in 2009, it is stated that: "Penetration testers found 763 high-risk vulnerabilities in 70 Web applications used for functions such as distributing communications frequencies for pilots and controllers to the public and other applications used for internal air traffic control systems within the U.S. Federal Aviation Administration."[150]

Less cyber and more physical would be the attack focused on radar or broadcasting systems, trying to either jam them or flood their receivers and thus disrupting their functionalities.[151] Pure cyber attack could try to make radar displays show imaginary planes in the ski thus creating false alerts. The option of targeting air traffic systems will be considered for the purpose of this analysis.

9.5.2.4. Physical attack alternative

Physical attackers may try to replicate the attacks from 9/11. In such case, the probability of success is much lower due to the surprise factor. Since 9/11, there have been very strict security procedures in place for the situation when control tower loses contact with a plane or when the plane deflects from its planned course. Smuggling weapons or explosives aboard of civil planes is also more difficult given the new security measures like whole body scans.

Attacker might try similar tactics as in the cyber attack alternative and focus on air traffic control systems. Destroying the control tower, servers running the system or damaging other critical components would cause difficulties for the pilots. For the purpose of this analysis only the alternative based on 9/11 attacks will be taken into consideration.

---

150 Federal Aviation Administration, *Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems,* (FAA, 2009), page 32, http://www.oig.dot.gov/StreamFile?file=/data/pdfdocs/ATC_Web_Report.pdf (accessed on 15th September 2013)

151 Paul Marks, *Air traffic system vulnerable to cyber attack,* (newscientist.com, 2011), http://www.newscientist.com/article/mg21128295.600-air-traffic-system-vulnerable-to-cyber-attack.html#.VGyzxskt1Gd (accessed on 17th September)

9.5.2.5. Conclusion and points

Criteria	Cyber Attack	Physical Attack
Insider information	3	8
Tools for attack	4	6
Possible damage	8	5
Physical presence	5	0
Probability of success	1	4
Total	21	25

Insider information is not really needed for the physical attack alternative. Of course, that the more information is known to the attacker, the higher is the probability to success, but only up to a certain extent. The attacker may decide to execute the attack disregarding the security measures. On the other hand, cyber attack alternative cannot be properly targeted without at least minimal knowledge of the target system. The amount of needed information depend on the type of the attack, but it will be always higher that in the case of physical attack.

Given the fact that air traffic control system is a special system not available to public, the attacker will have to program special malware or significantly customize available semi-products to prepare for the attack. The requirements for the cyber attack tools increase with the complexity of the attack. The procurement of needed tools will be easier if the aim is to create traffic overflow than when the attacker aims at taking over the control of the system. Presuming that sufficient tool for the physical attack alternative is a hand gun; it is very easy to get such equipment. Of course if explosives are to be used during the attack, the score for this criterion will be even lower.

It was presumed in the physical attack scenario, that the attacker can only target one plane at a time. The number of targeted plains cannot be larger than the number of attackers in an attack coherent with the 9/11 case. This premise is not valid for the cyber attack alternative. If the cyber attack shuts down radar, communication system or any critical component of the air traffic control system, it will influence all planes in range. Therefore the score for possible damage criterion is higher in case of cyber attack alternative.

Physical presence is necessary in the physical attack alternative. Cyber attack alternative may require the presence of the attacker in the premises of the target in only under special circumstances.

Probability of success is extremely low in the cyber attack alternative. The main problem of the cyber attack alternative is that even if successful, the pilots will still be in control of the plane and given their training should be able to safely land and minimize the damage. The situation might be worse for the pilots under difficult weather conditions or during low visibility, when they have to rely on information from plane computers. Physical attack alternative has still higher probability despite introduced security measures.

9.5.3. Tokyo sarin attacks

9.5.3.1. Case

In March 1995, five attackers released sarin in Tokyo subway system during the rush hour. The gas was in balls made of newspaper that were punctured in a given time in five different trains on the way to city center. The attackers left the trains immediately after releasing the gas. The trains continued on their way and distributed the gas at every stop. Despite the fact that the gas was not pure, it killed eight people and injured hundreds. Almost 5000 people were treated in relation to the sarin attacks.[152]

9.5.3.2. Comment

This case was already described above to illustrate how complicated is the process of manufacturing biological and chemical weapons. Tokyo underground case is very similar to the attacks in London, only the tools changes. Terrorists used explosives in London, chemical substance in Tokyo. The fact that the attacks in Tokyo were committed 10 years before the London attacks only proves that it is impossible to completely prevent attacks in public transport. This case is similar to the London attacks and will not be further analyzed, since the result would be very similar with the only difference in tools criteria.

---

[152] Kenneth Pletcher, *Tokyo subway attack of 1995,* (Britannica.com, 2014), http://www.britannica.com/EBchecked/topic/1669544/Tokyo-subway-attack-of-1995 (accessed on 5th March 2014)

9.5.4. Estonian case

In April 2007, the largest cyber attacks on public sector started when unknown attackers targeted the websites of political parties in Estonia. Before the end of the first week of attacks, the websites of main political parties in Estonia, government website and website of the Estonian parliament were knocked down by DDoS attacks.

During the following week the attackers targeted major Estonian news servers. At this time it was discovered that major of the attacking traffic was coming out of Estonia. News servers resorted to blocking all the traffic coming from abroad to slow down the traffic to at least partially restore their services.

The attacks continued for another two weeks culminating on 9th May, when Estonia witnessed the heaviest attack. At this time the hackers focused on the financial sector. In result the largest Estonian bank Hansabank had to shut down its Internet-based operations. There were severe consequences of this action. Firstly, approximately 97% of all banking transactions in Estonia are done online. Secondly, it severed the functionality of ATMs across Estonia. Thirdly, Estonian debit cards stopped working outside the country.[153]

9.5.4.1. Comment

The Estonia case is actually the only known example when cyber attacks of a large scale managed to substantially disrupt the everyday life in a country. The attacks targeted various different targets including financial institutions, government web pages and many other sites. In the end, Estonian authorities managed to repel the attackers at the cost of shutting down targeted systems for necessary period of time. Probably the most serious impacts of the attacks were those related to the banking sector, because they have direct influence not only on the national economy, but also on the citizens of Estonia. Had the

[153] Jason Richards, *Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security,* (Elliot School of International Affairs, 2007), http://www.iar-gwu.org/node/65, (accessed on 5th October 2013)

problems of banking sector lasted longer, the lack of liquidity without proper governmental response might have resulted in civic unrest.

The attacks provoked increased interest in the cyber security and related risks and initiated the foundation of NATO Cooperative Cyber Defense Centre of Excellence in Tallinn focused on research in the domain of cyber security.

Cyber attacks in this case were clearly provoked by the actions taken by local authorities. Despite the accusations made by Estonian representatives, there is no proof that Russia was behind these attacks. This only highlights the problem of attribution in cyber space.

The focus will be on the attacks on the banking sector for the purpose of this analysis.

9.5.4.2. Cyber attack alternative

Cyber attack alternative would be similar to the described case. The main feature of Estonian attacks is the scale. The attacks simultaneously targeted several institutions and each attack was executed by large botnets. This combination of factors makes cyber attacks very difficult to defend against. Of course that there is always the last resort action – "switching off the Internet." But even this is not always completely possible. Consequences of such action could also be worse that the attacks themselves. Another important feature is the selection of targets and the impact of the attack. Attackers focused on Hansabank, the largest bank in Estonia. Given the fact that the concentration of the banking market in Estonia is very high (70% in 2011),[154] attacking Hansabank was sufficient to actually cause severe problems to whole banking industry if successful.

In order to achieve similar results as in this case, the attackers would have to prepare several large botnets located in different countries using different paths and servers to actually reach their targets. Using botnets located across the globe would make it harder to identify the source of the attack and to simply cut off one particular source of attacks from

[154] OECD, *Estonia, Review of the Financial System,* (OECD, 2011), page 21, http://www.oecd.org/finance/financial-markets/49497930.pdf (accessed on 11th October 2013)

the target. If executed properly with sufficient resources, DDoS attacks have a very high probability of success.

Attackers would also have to target either a country with highly concentrated banking market or target simultaneously several targets to reach the same impact as in this case. The impact of successful attacks on banks has exponential effects – the longer the bank operations are not functional, the worse is the situation. If the attackers manage to successfully attack a bank having impact on 70% of the market in a developed economy where majority of transactions is done online and the amount of used liquidity in transactions is very low, in couple of days the situation will become critical.

9.5.4.3. Physical attack alternative

Physical attack alternative on such a large scale is practically impossible. Even if the attackers would focus on the banking sector, they would have to physically take over the control of the banking core system to actually prevent other branches from operating. Other possibility for the physical attack scenario would be to damage or destroy infrastructure needed for financial infrastructure processing.

9.5.4.4. Conclusion and points

Criteria	Cyber Attack	Physical Attack
Insider information	6	6
Tools for attack	5	3
Possible damage	8	6
Physical presence	9	0
Probability of success	3	2
Total	31	17

Needed amount of insider information is in both alternatives relatively low. It is easy to find out which banks have targeted market share and where is the central building of the bank. It might be slightly more difficult for the physical alternative to find out where key servers or other infrastructure are located. Cyber attack alternative using DDoS types of attack only needs to know which websites are to be targeted. It is easy to identify public gateways for login into online banking. It will be more difficult to identify websites used for communication among banks, but this is still not an impossible task. Obviously, knowing more about security measures and procedures used in the targeted bank would increase the probability for success, but such information is not needed to actually launch the attack.

Cyber attack alternative relies on the usage of botnets. Originally, attackers had to prepare the botnets themselves. This included infecting computers with needed malware, installing Troyans to gain control over the computer without anyone noticing, setting up false servers to control the botnet and other activities. But approximately from 2003,[155] hackers started to make botnets not for particular action, but for financial gain. Botnets can be bought online or only rented for needed time. In 2012, the price in Russia for a botnet of 2000 bots was 200 USD, renting botnet for DDoS attack cost from 30 to 70 USD per day.[156] Even if the prices slightly increased, buying or renting botnets to present a real threat is still very

[155] McAfee, *Global Security Threats and Trends,* (McAfee, 2006), https://mcafee.imiinc.com/nai7588/aug06/article3.jsp (accessed on 11th October 2013)
[156] Ian Steadman, *The Russian underground economy has democratized cybercrime,* (wired.co.uk, 2012), http://www.wired.co.uk/news/archive/2012-11/02/russian-cybercrime (accessed on 21st September 2013)

affordable when compared to physical attack alternative, which needs weapons, explosives and other materials.

Possible damage in this case depends on the market share of the bank, on the time for which the bank cannot operate and on the cyber dependency in given country. If the vast majority of transactions is done online, the attacks will have major consequences. The effects of the attack will come in force in the moment that the clients of the bank run out of cash. When ATMs are out of order, the only option is to visit the bank and to withdraw the money. Presuming that the core banking system is still functioning and it is possible to actually access the system for withdrawal, the only problem is the availability of cash in the bank. Theoretically, this kind of cyber attack might result in a run on the bank, but only under specific circumstances. Successful attack would also influence private sector. Companies might find themselves in the state of insolvency. Given the fact that current banking systems rely on cyber space and online communication, successful attack de facto isolates the bank from the network. Whereas physical attack can achieve the same results only if necessary infrastructure is destroyed and the replacement will take too much time.
Physical presence is not needed in the case of cyber attack alternative. However, it is essential in the physical attack scenario. Sometimes it may occur that critical infrastructure is backed up or located in different cities or even states.

Probability of success in the physical attack scenario is relatively low. The attack would have the same consequences as the cyber attack alternative only if the bank had the entire critical infrastructure located in one place. But since this would be against security principles, it is highly improbable. If the attackers have to focus on several targets, the probability of success decreases. Another problem is the fact that destroying the infrastructure is not sufficient. The attackers would also have to prevent restoration of the hardware. On the other hand, cyber attackers simply redirect their botnets to a different address. If the attackers dedicate necessary resources, it is very probable that the administrators would have no other option then to shut the web page down, if only for a couple of minutes. Of course that such a short disruption would not cause severe problems, but DDoS attacks can last several days even weeks as in the Estonian case. However, it is

necessary to presume that security measures in banks and in financial sector generally have been significantly improved as the cyber security risks increased in importance. Security measures might not prevent the DDoS attacks, but they can mitigate the consequences. Therefore the probability of success of the same level as in the Estonian case is higher than in the physical attack alternative, but still relatively low.

9.5.5. Virus attacking military drones

9.5.5.1. Case

In 2011 journalist published information that military drones were infected by a computer virus. The infection involved the Predator and Reaper drones operating in Afghanistan and in other conflict zones. Despite several attempts to remove the virus from the system, many drones remained infected. So far no security issues related to this infection have been reported. Nevertheless, the specialist confirmed that the virus hit both classified and unclassified machines at Creech Air Force Base in Nevada and therefore it is not possible to completely reject the hypothesis that the virus might have transmitted some sensitive data over Internet to remote computers

Despite the increased role of military drones for the U.S. military, the drones are known to have security flaws. Another example is the transmission of video from the drones. The transmission is not always encrypted and in 2009 American forces discovered in Iraq huge amount of decoded video recording from the drones in the computers of Iraqi insurgents. Later it was found that cheap software was sufficient to enable eavesdropping the transmission from drones to the operators.[157]

[157] Noah Shachtman, *Exclusive: Computer Virus Hits U.S. Drone Fleet,* (wired.com, 2011), http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/ (accessed on 17th September 2013)

9.5.5.2. Comment

There have been no reported consequences of the virus infecting military drones so far. However, increased usage of military drones as well as their modernization raises questions about related risks.[158] Obviously, some types of drones are equipped with missiles and if the hackers manage to gain control over such drone, they will have weaponry that is under current circumstances inaccessible to them. The case will not be further analyzed as its sole purpose is only to illustrate the security risks related to the usage of drones.

Some companies are actually considering using civil version of drones in their business activities according to recently published information.[159] Of course that real usage of drones in cities is rather theoretical; it raises questions related to the security of such drones. These concerns were only increased by publishing Skyjack. Skyjack is a name for hacking a drone and using it to take control of other drones using their wi-fi connection. The author of the process how to gain control of a drone using different drone is Samy Kamkar. Mr Kamkar is famous for his worm that he released into MySpace in 2005, for which he was banned by American court from using computers for three years. In 2013 Mr Kamkar demonstrated that it is possible to actually hack a civilian drone.[160] Despite the fact that army representatives deny any possibility that military drones can be hacked in a similar way, the case of a drone lost over Iran raises doubts. In the Iranian case, American surveillance drone was captured by Iranian forces. While the U.S. Army claimed that they lost control of the drone and therefore it crashed,[161] Iranian army stated that they made

---

158 Katia Moskvith, *Are drones the next target for hackers?,* (bbc.com, 2014), http://www.bbc.com/future/story/20140206-can-drones-be-hacked (accessed on 5th June 2014)

159 For instance: Sarah Perez, *Facebook Looking Into Buying Drone Maker Titan Aerospace,* (techcrunch.com, 2014), http://techcrunch.com/2014/03/03/facebook-in-talks-to-acquire-drone-maker-titan-aerospace/ (accessed on 5th June 2014)

160 Jordan Crook, *Infamous Hacker Creates SkyJack To Hunt, Hack, And Control Other Drones,* (techcrunch.com, 2013), http://techcrunch.com/2013/12/04/infamous-hacker-creates-skyjack-to-hunt-hack-and-control-other-drones/ (accessed on 18th May 2014)

161 Ynet, *US official: Iran assembled drone like puzzle,* (ynetnews.com, 2011), http://www.ynetnews.com/articles/0,7340,L-4162745,00.html (accessed on 5th June 2014)

the drone land thanks to the activity of their cyber warfare unit.[162] The fact is that Iran showed pictures of undamaged drone and American officials in the end confirmed that it was indeed an American drone.[163]

The intended introduction of unmanned vehicles to prevent casualties in the military ranks is a logical consequence of the technical progress and political pressure. But responsible authorities have to pay attention to security aspects of these vehicles. This case also illustrates that despite the level of implemented security measures, the human error cannot be avoided – in this case using was probably military computer used for playing Facebook games.

[162] Scott Peterson, Payam Faramarzi, *Exclusive: Iran hijacked US drone, says Iranian engineer,* (csmonitor.com, 2011), http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video (accessed on 5th January 2012)

[163] Bob Orr, *U.S. official: Iran does have our drone,* (cbsnews.com, 2011), http://www.cbsnews.com/news/us-official-iran-does-have-our-drone/ (accessed on 5th February 2012), Wire Staff, *Obama says U.S. has asked Iran to return drone aircraft,* (cnn.com, 2011), http://www.cnn.com/2011/12/12/world/meast/iran-us-drone/ (accessed on 5th February 2012)

9.6. Summary

The scores for particular aspects of both variants are displayed in the following chart.

	Row Labels	Grand Total	Insider information	Physical presence	Possible damage	Probability of success	Tools for attack
9/11 attacks	Sum of Cyber Attack	21	3	5	8	1	4
	Sum of Physical Attack	24	6	0	5	5	8
Bellingham Gasoline Pipeline	Sum of Cyber Attack	27	3	7	6	3	8
	Sum of Physical Attack	23	6	1	6	8	2
Browns Ferry nuclear plant	Sum of Cyber Attack	24	1	5	9	2	7
	Sum of Physical Attack	21	4	1	9	5	2
Davis – Besse nuclear plant	Sum of Cyber Attack	21	2	6	3	4	6
	Sum of Physical Attack	0	0	0	0	0	0
Disinformation and its impact on financial markets	Sum of Cyber Attack	32	6	9	8	4	5
	Sum of Physical Attack	20	5	1	6	2	6
Estonian case	Sum of Cyber Attack	32	6	9	8	4	5
	Sum of Physical Attack	17	6	0	6	2	3
JPMorgan card data loss	Sum of Cyber Attack	20	6	5	3	2	4
	Sum of Physical Attack	0	0	0	0	0	0
London underground bombing	Sum of Cyber Attack	23	3	4	8	2	6
	Sum of Physical Attack	26	9	0	7	7	3
Maroochy Water Services	Sum of Cyber Attack	24	2	6	8	3	5
	Sum of Physical Attack	24	8	1	4	7	4
South Korea cyber attacks	Sum of Cyber Attack	38	8	9	9	4	8
	Sum of Physical Attack	23	3	3	6	3	8
Total Sum of Cyber Attack		262	40	65	70	29	58
Total Sum of Physical Attack		178	47	7	49	39	36

It is understandable that the cyber attack alternative has in total significantly higher score. This difference can be partially explained by the fact that for two cases the physical attack alternative is not feasible. Disregarding the points related to these two cases, the cyber attack alternative has still higher score, but now it is 221 making the difference 43 points. The biggest difference in points between the alternatives is in the case of physical presence criterion. Physical presence is regarded in the analysis as a negative aspect. If the attacker is forced to be physically present, it increases the chances of being captured by police or by other security forces. Nevertheless, it is a question if the understanding of this aspect is not wrong in this analysis. Of course, this criterion demonstrates the global aspect of cyber space. But the physical presence is inevitable in case of suicide attacks. This type of attacks is usually religiously motivated. The question is, whether without the self-sacrifice and the prospect of reward in the afterlife terrorist organizations of religious nature would have the same number of volunteers.

Accepting the premise that physical presence of the attacker is not a disadvantage in case of physical attack alternative and deducting the points for this criterion, the physical attack alternative has slightly higher score – 171 versus 167 points for the cyber attack alternative.

	Grand Total	Insider information	Possible damage	Probability of success	Tools for attack
Total Sum of Cyber Attack	167	32	64	23	48
Total Sum of Physical Attack	171	47	49	39	36

Despite the very close final results, the distribution of points rather different. Insider information criterion presents an advantage for the physical attack alternative. Only in one case (disinformation) were the awarded points higher for the cyber attack alternative. Insider information is a general Achilles heel for the cyber attack. When the cyber attack is to be under the control of the attacker or there is a strict plan that has to be followed, the attacker needs too much insider information. This is nicely described in the Stuxnet case. This attack was very precise, but the amount of used insider information is too high to believe that similar action could be reproduced by a terrorist group. However, this statement does not exclude the availability of such information per

se. As it was already discussed, the amount of information that can be abused by the attacker is increasing directly with the usage of ICTs and cyber space in all domains of everyday lives. And so is increasing the number of individuals in possession of such information or having access to such information. The attacker does not have to be former employee as in the Maroochy case, but also this tendency of a revenge motive has to be taken into consideration. On the other hand, if the attacker simply launches a general attack, e.g. virus, without particular target in mind, he might in the end attack systems in banks, nuclear plants or in other parts of national critical infrastructure. In this case, the attacker does not need any insider information from particular institutions, but is he cannot be in control of the attack neither be aware of possible consequences this attack will have. Ironically, some attacks in the history with serious consequences were simple mistakes, as in the Morris worm case in 1988.[164]

Possible damage criterion final score is in favor of cyber attack. Cyber attack generally scores higher than the physical attack scenario or receives at least the same number of points. There are two main reasons for this result.

Firstly, it is the network aspect. In cases where the target is actually in a form of network, like pipeline network, underground network, distribution networks, bank network, etc., the cyber attack targets the system which is in charge of the whole network. Therefore if the attack is successful and targeted system is out of order or under the control of the perpetrator, it directly influences the whole network disregarding physical location of particular components. Disrupting the functionality of control system in a gas pipeline network may influence the whole network, whereas in the physical attack scenario, the target is always one subject. Of course that even the physical attack might have similar network consequences, but only under special conditions, e.g. destroying critical nod or critical part of the infrastructure. But in such case the attacker would need to get access to key insider information.

Secondly, even if the attacker manages to destroy critical part of infrastructure with the network effect, the system controlling the network will trigger security mechanisms and

[164] U.S. Court of Appeals, *USA v. Robert T. Morris,* (U.S. Court of Appeals, 1991), No. 774, Docket 90-1336. http://www.loundy.com/CASES/US_v_Morris2.html (accessed on 9th January 2014)

will mitigate the attack. On the other hand, if the system is corrupted or under hostile control, the administrators are in a much worse situation, as they have to fight their own system. It is true that still manual override of the system's order should be possible to mitigate the consequences of the attack. However, such manual alternatives present additional costs and there might be the tendency to rely completely on modern technologies without manual control options. This manual "last resort" procedure might not be possible in cases when virtual assets are targeted. This applies mainly to the financial sector, when practically all data are kept in a virtual form.

Probability of success favors the physical attack alternative. This criterion is closely related to the possible damage. It is possible to simplify the formulation stating that physical attacks targeting individual targets have higher probability, but cyber attacks with lower probability of success can cause more damage. The score for this criterion reflects the asymmetrical nature of terrorist attack. Despite increased security measures, the attacker can always find a target with weaker protection, thus increase his chances on success. Carefully planned and aimed cyber attacks will usually target important systems. Owners of such systems are aware of the importance and will try to ensure maximal security to prevent cyber attacks. Given the fact that cyber attacker will need a lot of insider information to prepare the attack, he may not be aware of all security procedures and even if partially successful, the final goal might not be achievable. If the cyber attacker does not focus on a particular target and aspires to exploit a security whole in some component or system in general, he can successfully attack also parts of the critical infrastructure. The reason is that in such case the asymmetric aspect of terrorism will apply. The attacker does not target the critical system, which is well protected. But he might disrupt functionality of one small component with coincidental disastrous consequences to the whole system. This can be observed in the nuclear plants' cases, where the incidents started with malfunctions of "forgotten components." The risk is that administrators focus on the protection of critical system and omits other components or secondary systems that might in the end influence the functionality of the primary systems.

Tools for attack criterion final score ended in favor of cyber attack alternative. This is due to the fact that there are no measures to regulate the proliferation of "cyber

weapons." Pieces of code, semi-finished malware, and other tools needed for cyber attacks can be procured over the Internet on a global level, theoretically without any risk. The final preparation of the software requires certain level of IT skills, but such resources can be hired or educated. On the other hand, previous terrorist attacks often used explosives or weapons. Security measures were introduced in order to monitor any attempts to manufacture explosives at home or to prevent individuals from taking weapons or explosives aboard on planes or underground trains. In some states needed tools can be procured more easily, but still it will be more difficult for the physical attack alternative than for the cyber attack alternative.

Based on the research results, it is possible to reject the initial hypothesis that cyber attack alternatives will score significantly lower than physical attack alternatives.

9.7. Who will unleash cyber attacks?

The analysis of case studies revealed that the attackers either need significant amount of insider knowledge to prepare well aimed attack or their action will rely on pure force and scale of the attack. Current terrorist group as discussed in previous chapters have not attempted to commit significant cyber attack so far or it has not been successful. The question is, whether terrorist groups currently acting against the United States will change their tactics and embrace new technologies also for the purpose of terrorist attacks. The number of terrorist attacks against American targets in the United States has significantly decreased in past years. On the other hand, the attacks in the rest of the world against American targets have increased and their nature has not significantly changed. Suicide bombers, booby traps, mines or snipers regularly endanger American forces in Afghanistan and Iraq. It seems improbable that the terrorists will change their tactics in this region when their actions are relatively successful. It is a different situation for terrorist attempts in the United States. The change of tactics towards cyber space might improve their chances, but would it help to attain their strategic goals? Destabilizing financial sector or causing incident in a nuclear facility would definitely increase the prestige of the terrorist group and probably would also bring attention of media to the ambitions of the terrorist group. But only few types of cyber attacks will cause casualties and actual physical damage. The cyber attacks do not require martyrdom. Therefore current terrorist organizations ranked as Islamist fundamentals

might not be so willing to try new technologies in this way; as such actions are too remote from their actual goals[165] and would distract them from their local actions.

On the other hand new group of potential terrorist emerged together with the increase of use of cyber space and modern technologies. Before the introduction of World Wide Web, only people with programming and IT skills could benefit from the cyber space. The number of users is increasing and so is the usage of cyber space. Hand in hand with the usage comes the regulation. The control and regulation of cyber space is motivated also by the economic effects of the cyber space and by the emerging dependency on the cyber space and modern technologies. Such actions disturb the community of IT experts who were used to be independent and untouchable thanks to their unique and deep knowledge of IT. These people would never plant an explosive or commit a suicide attack. But they will fight for what they see as their rights regarding cyber space. And naturally they will choose cyber attacks to reach their goals. Probably the most know example of such mobilization is the group Anonymous discussed in previous chapters.

More determined and better equipped are the groups of attacker sponsored by states. State sponsored terrorist groups or semi-organized groups with adequate skills actually present more significant threat regarding cyber attacks.[166] Actions of terrorist groups supported by states will not differ much from actions of other terrorist groups. They might have better equipment and targets more in line with the need of the state, but it is still a terrorist organization. But some states have at their disposition semi-organized groups of experienced hackers or even specially trained units.[167] Attacks against Estonia, Stuxnet or Flame malware are some of the actions attributed to this type of attackers. The question is whether such actions can be labeled as terrorist cyber attacks. Indeed they are cyber attacks, but these actions often lack some of the characteristics of

---

[165] Max Abrahms, *The Political Effectivness of Terrorism Revisited*, (Comparative Political Studies, 2012), http://cps.sagepub.com/content/45/3/366 , page 364 (accessed 21st November 2013)

[166] For instance Kenneth Geers, et al., *World War C : Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks,* (FireEye, 2014), http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf (accessed on 15th September 2014), Steve Ranger, *Hostile state-sponsored hackers breached government network,* (ZDnet.com, 2014), http://www.zdnet.com/hostile-state-sponsored-hackers-breached-government-network-7000030619/ (accessed on 14th September 2014)

[167] National Cyber Security Centre, *Cyber Security Assessment Netherlands CSAN-3,* (National Cyber Security Centre: Netherlands, 2013), pages 8-10, https://english.nctv.nl/Images/cybersecurityassessmentnetherlands_tcm92-520108.pdf?cp=92&cs=65035 (accessed 5th May 2014)

terrorist acts, for instance motivation. These actions could be labeled as acts of war or at least hostilities between countries, were it not for the attribution problem. It is very difficult to identify the perpetrator of the attack in the cyber space. The assurance in cyber attack attribution is not higher than 60% in the United States,[168] which is not enough for officially declared retaliation. State sponsored actions usually focus on intelligence gathering or industrial espionage.[169] However, state sponsored units have far better resources than ordinary terrorist groups or "new terrorists" to perform successful cyber attack with serious consequences.

It is therefore necessary to focus not only on the possibility of current terrorists attempting to commit a cyber attack, but on the cyber security**.**

168 Said by Alexander Klimburg during Prague Transatlantic Talks 2014: Facing the Atnalntic Cyber Challenge Conference held in Prague, 28th – 29th May 2014. Alexander Klimburg is a research fellow at Belfer Center for Science and International Affairs, Cambridge/US.

169 National Cyber Security Centre, *Cyber Security Assessment Netherlands CSAN-3,* (National Cyber Security Centre: Netherlands, 2013), pages 8-10, https://english.nctv.nl/Images/cybersecurityassessmentnetherlands_tcm92-520108.pdf?cp=92&cs=65035 (accessed 5th May 2014)

10. Current position of the U.S. as a superpower in cyber space

The U.S. has strengthened their position of global superpower during the Cold war. Despite the fact that the defense budget was lowered after the collapse of the Soviet Union, it is still among the highest in the world reaching slightly over 600 billion USD.[170] Significant share of this amount is dedicated to the modernization of the army and to the implementation of modern technologies. Modern technologies in the army enables more efficient management of military operations, improves the communication and mainly help to reduce the number of casualties in the U.S. Army. The U.S. is currently the only state that is capable of conducting military operations anywhere in the world. Recent conflicts in Afghanistan and Iraq have demonstrated the supremacy of American forces on all battlefields – on the land, in the air and at the sea. Generally the supremacy in the air allows minimize the risk for the ground forces, which are supported by the naval forces. American strategy strongly relies on the modern technologies, which enables precise navigation and communication on long distance, thus enhancing the effectiveness of the conventional weapons.[171] The U.S. is up to a certain extent militarily dominant in the space as well. Even if the original plans of star wars from the era of Reagan government; including the Initiative of strategic defense,[172] have not been executed. However, current dominancy of the U.S. in the space might change with regards to the recent Chinese exploration of the space.[173]

Military experts have relatively recently shifted their attention to a new dimension for the warfare – cyber space. Apart from traditional battlefields, cyber space was artificially created by men. It is made up by all computers, systems, machines and other objects sharing information using Internet or any other network. The question is, whether this new dimension might change current status quo of the U.S. as the only true geopolitical superpower. This chapter analyses the position of the U.S. in cyber space compared to

170 "DOD Releases Fiscal 2013 Budget Proposal," Department of Defense official web pages, http://www.defense.gov/releases/release.aspx?releaseid=15056 (accessed on 2nd August 2012)
171 For instance modern systems of targeting, nocturne vision, ETA.
172 BBC News, *1983: Reagan launches Cold War into space*, (BBC Home: London, 1983), http://news.bbc.co.uk/onthisday/hi/dates/stories/march/23/newsid_2794000/2794525.stm (accessed on 15th August 2012).
173 Tania Branigan, *Chinese astronauts complete successful docking at space lab,* (The Guardian: London, 2012), http://www.guardian.co.uk/world/2012/jun/18/chinese-astronauts-complete-space-docking (accessed on 8th September 2012)

other states in order to reject or confirm the hypothesis that the U.S. have a superior position in cyber space.

10.1. Methodology

Comparative analysis cannot be used in this case because of several reasons. Firstly, it is not possible to simply derive the ability from the number of dedicated personnel. In case of cyber war, the qualitative aspect is much more important than the quantitative aspect. Significantly larger number of specially trained soldiers can be defeated by single skillful attacker. Of course, the superiority of numbers has some importance, but it is not decisive. This problem is valid also for the comparison of conventional armies, where other factors than mere numbers have to be taken into consideration.[174] Secondly, it is necessary to have sufficient amount of reliable data for this kind of comparative analysis. In case of units focusing on cyber space, such numbers are often confidential, therefore not public or rather ambiguous.

Dedicated budget could serve as a mean of comparison. Despite the fact that American defense budget is the largest in the world, it does not mean that the funding of cyber related units and programs is the largest one. It is possible to compare the defense budgets of particular countries, but it would be significantly more difficult to get access to the size of budget dedicated to the cyber war. Moreover, the national capability might not be concentrated under the Ministry of Defense or the Army. It might happen that in some countries it is the secret service responsible for the domain of cyber space. There for it is impossible to acquire comparable data without detailed knowledge of the responsibilities of particular offices and ministries. In the end, the comparison based on the size of budget would not be sufficiently reliable. As in the case of the size of dedicated units, mere numbers are not decisive, as the funds might be inefficiently distributed. Financial resources are closely related to the available equipment. Nevertheless, the specification of equipment used in particular countries for the research or for proactive defense in cyber space cannot be acquired. Even if such data were available, the equipment is not the decisive factor. The worst viruses were usually

[174] For instance hypothesis stating that two armies are equally strong based on the same numbers of tanks.

programmed using ordinary PC. Neither it is possible to compare the destructive power of particular countries. There are no missiles to be counted.

One of the reasons, why the information is so scarce, is the tactical advantage. Any proclamation about the cyber attack capabilities or cyber defense perfection might provoke a reaction. Official proclamation about the impenetrability of national network might result in large number of probing attacks even from non-state actors, like hackers. Boasting about national capabilities to penetrate particular systems might persuade other parties to change their operational systems. Stating the fact that national banking system is not safe enough would only disrupt the trust of public and point out possible targets for the adversaries. That is why there is so little reliable information about the cyber security and cyber attack potential.

Since the data and detailed information are so scarce or completely inaccessible, the comparative analysis is based on the comparison of relative potential with reference to other states included in the analysis. The relative advantage or disadvantage is expressed in the form of points, where 0 is minimum and 10 is the maximum value. The analysis is based on the approach used by Richard A. Clarke in his book Cyber War.[175] This publication is one of the few available that describes also the political aspects of cyber conflict. The main goal of this book is to point out possible vulnerabilities of the U.S. in terms of dependency on modern technologies in combination with low defense capabilities. The author combines his personal experience from national security service with his knowledge of internal processes in the highest levels of the American administration to point out possible shortfalls of the cyber security in the U.S. Richard A. Clarke briefly analyzed three aspects related to cyber war. He analyses the ability of a state to commit attack in cyber space (attack capabilities), the ability to proactively defend national assets in cyber space (defense capabilities) and finally the dependence of given state on cyber space and on related technologies (dependency). For the purpose of this dissertation, same characteristics and the same set of national states were chosen in order to compare final results and to demonstrate the recent development in this field. For each characteristic, two national states are always compared and using deduction and the transitivity final score is derived. Analyzed states are: U.S., Russia,

[175] Richard A. Clarke a Robert K. Knake, *Cyber War,* (HarperCollins: New York, 2010)

China, Iran and North Korea. The set of states includes traditional rivals in terms of global superpower as well as states, which might have sufficient motivation to take advantage of potential supremacy in cyber space.

10.2. The attack capability

The ability to execute an attack in cyber space means that the units are able to overcome security measures of the target and put it out of service or to take control of the target. The attack may result in the data alternation or deletion, or might be part of larger scale operation. The target can be a network, particular system or computer. The nature of the system is not distinguished – it might be a military system as well as private company network.

10.2.1. The attack capability of the U.S.

It is essentially the capability to attack that got the attention of the army first. Therefore specialized units responsible also for conducting cyber attacks were founded independently in every army resort and only later they were organized under common command.

10.2.1.1. Air force cyber units

The U.S. air forces have the cyber units organized under the 24th Air Force based in Texas. It consists of three units – 67th Network Warfare Wing, 688th Information Operations Wing and 689th Combat Communications Wing.

67th Network Warfare Wing manages, trains and equips cyber warfare units for the combat, defense and other usage of cyber space. It is also responsible for the network operations, training, tactics and air force cyber unit management.[176]

688th Information Operations Wing provides necessary infrastructure and trained personnel for the integrated units in cyber space.[177]

[176] „67th Network Warfare Wing," official web pages of this unit, http://www.24af.af.mil/units/67nww.asp (accessed on 5th August 2012)
[177] „688th Information Operations Wing," official web pages of this unit, http://www.688iow.af.mil/ (accessed on 6th August 2012)

689th Combat Communications Wing is responsible for the training of personnel able to install and operate communication links, air traffic systems and other systems for military and civilian usage under any conditions anywhere in the world. Special tactical skills of soldiers from this unit enable them to be part of standard military operations. In case of joint operations, they can effectively provide communication network implementation and also fulfill other combat tasks.[178]

There are approximately 16000 military and civilian personnel in the Air Force cyber units, but only 6-8000 soldiers specially trained for cyber attacks (67th Network Warfare Wing).[179]

10.2.1.2. US NAVY cyber units

From the perspective of the US NAVY, soldiers trained also in the information technologies and in cyber space are organized under the 10th Fleet, NETWARCOM (Naval Network Warfare Command). This unit is responsible for the management and maintenance of US NAVY networks, takes part in common operation with other units. [180] Given the nature of the tasks this unit is responsible for, the total number of specially trained soldiers is probably lower than in case of the Air force units.[181] However, the proposed optimal number of the unit personnel is approximately 14 000.

10.2.1.3. Land forces cyber units

Specially trained troops within the land forces are organized under the lead of the U.S. Army Cyber Command. The U.S. Army Cyber Command plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyber space operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyber space and deny the same to adversaries. [182] The U.S. Army Cyber Command capitalizes on existing Army cyber resources and improves operational readiness by bringing Army cyber resources under

---

178 „689th Combat Communications Wing," official web pages of this unit, http://www.24af.af.mil/units/689ccw/index.asp (accessed on 7th August 2012)
179 Ibid.
180 „Naval Network Warfare Command," official web pages of this unit, http://www.netwarcom.navy.mil/ (accessed on 7th August 2012)
181 Richard A. Clarke a Robert K. Knake, *Cyber War,* (HarperCollins: New York, 2010), page 43
182 „Army Cyber," U.S. Army Cyber Command official web pages, http://www.arcyber.army.mil/org-uscc.html (accessed on 7th August 2012)

a single command. The Network Enterprise Technology Command/9th Signal Command (NETCOM) and 1st Information Operations Command are subordinate units to Army Cyber Command.[183]

NETCOM headquarters is based in Arizona and it is the single information technology service provider for all network communications. NETCOM is also responsible for the security, accessibility and maintenance of army network on the national and international level. These activities are provided thanks to nearly 16000 soldiers, civilians and contract personnel.[184]

1st Information Operations Command provides support operational teams responsible for the planning of informational support and specialized actions (e.g. propaganda, disruption of target system and networks). They also run the CERT for the U.S. Army.[185] The U.S. Intelligence and Security Command (INSCOM) is an Army major command that conducts intelligence, security and information operations for military commanders and national decision makers.[186]

10.2.1.4. Organization of the U.S. attack forces

The U.S. Cyber Command presents the highest level of command of the cyber units. It is partially subdued to the Strategic Command (STRATCOM). The director of the NSA is in the same time a four star general and the highest commander of American cyber command. This situation resulted from negotiations between the army and agencies responsible for the management of the American cyber space.[187] The core of the dispute was related to the development of interest in cyber space of particular agencies and units, since in the beginning only the security agencies had necessary equipment and experience to be active in cyber space. Firstly the have been collecting necessary information, but the scope of activities have significantly grown during last twenty

[183] Army Cyber," U.S. Army Cyber Command official web pages, http://www.arcyber.army.mil/org-uscc.html (accessed on 7th August 2012)
[184] „U.S.Army Network Enteprise Technology Command," official web pages of this unit, http://www.army.mil/info/organization/unitsandcommands/commandstructure/netcom/ (accessed on 7th August 2012)
[185] „1st IO Command," official web pages of this unit, http://www.1stiocmd.army.mil/ (accessed on 8th August 2012)
[186] „United States Army Intelligence and Security Command," official web pages of this unit, http://www.inscom.army.mil/ (accessed on 8th August 2012)
[187] Richard A. Clarke a Robert K. Knake, *Cyber War,* (HarperCollins: New York, 2010), Franklin D.Kramer et al., eds., *Cyberpower and National Security* (Potomac Books: Dulles, 2009)

years. On the other hand, in the same time when security agencies had specialized teams, the army was establishing dedicated units. Nevertheless, only the army units are supposed to conduct military actions in cyber space.

10.2.1.5. Additional attack capacities

Apart from the military units it is highly probable that also governmental agencies like NSA, CIA and FBI possess necessary resources to execute offensive actions in cyber space. However, the primary role of the agencies is to collect information and no to perform offensive actions.

There are also a significant number of private companies employing experts in the cyber security field. Theoretically they might take part in the cyber conflict. Nevertheless, their participation in offensive actions is very unlikely. It is necessary to mention also semi-organized groups of hackers. Their offensive potential might be used if there is a common case and possible way how to cooperate with the official representatives (such utilization of hackers is more frequent in other states, see below).

10.2.2. The attack capability of other countries

It is very difficult to assess the number of specially trained soldiers in other countries due to the lack of official resources. Nevertheless, it is possible to note that all countries selected for this analysis have a special program related to building cyber space offensive and defensive capabilities.

The existence of the "Blue team" in China has been officially confirmed in 2011. It was the speaker from the Ministry of Defense who mentioned the existence of specially trained unit. However, the total number of military or civil units specialized in cyber space actions is unknown, as well as their organization.

Based on the indirect evidence, it is logical to assume that on certain cyber attack Chinese hackers cooperate with the responsible state agency. It is impossible to decide how the state is involved in such actions or if such activities are only tolerated.[188] It is a

[188] For instance: Sean Gallagher, *Chinese hackers steal Indian Navy secrets with thumbdrive virus*, (arstechnica, 2012), http://arstechnica.com/security/2012/07/chinese-hackers-steal-indian-navy-secrets-with-thumbdrive-virus/ (accessed 9th August 2012), Michael Riley, Dune Lawrenc, *Hackers Linked to China's Army Seen From EU to D.C.*, (Bloomberg News, 2012), http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html (accessed on 9th August 2012), FoxNews, *Chinese hackers took over NASA's Jet*

fact that cyber attacks tracked to servers or computers located in China remain unsolved due to the unwillingness of Chinese authorities to cooperate.

There is practically no official information or confirmation of existence of specialized units dedicated to the actions in cyber space. Therefore it is impossible to determine the size of such units or their organization. In case of Russia, there are likely several groups of semi organized hackers who cooperate or at least support actions in cyber space executed in line with the foreign policy of Russia; for example the cyber attacks aimed at Estonian cyber space in 2007 or similar actions in South Ossetia in 2008. There is literally no information on the Iranian specialized forces, but it is very probable that the Iranian government have increased their cyber capabilities if only due to the Stuxnet virus. Some security experts raised concerns about the growing offensive potential of Iran.[189] There is only scarce information about the organization of North Korea army; neither there is any official information on North Korean cyber units. However, some security experts and American representatives raised concerns about their offensive capabilities. [190] Rumors have it that North Korean offensive unit is actually located in Shanghai.

10.2.3. International comparison

As already discussed in the methodology part, the comparison of cyber space capabilities is very difficult. In it very difficult especially for the offensive potential, since there are only few precedents demonstrating the possibilities cyber space offers; for example the logical bomb, [191] which was allegedly implemented by CIA into the system managing gas pressure in the pipelines. This software was manipulated on purpose and intentionally left to be accessed by Russian spies. The software was installed in Russia and the logical bomb triggered in 1982, leading to the strongest non-nuclear explosion

---

Propulsion Lab, Inspector General reveals, (FoxNews.com, 2012), http://www.foxnews.com/scitech/2012/03/01/chinese-hackers-nasa-jpl-lab/#ixzz24kilV9N9 (accessed on 10th August 2012)

189 Tom Gjelten, *Could Iran Wage A Cyberwar On The U.S.?*, (National Public Radio, 2012), http://www.npr.org/2012/04/26/151400805/could-iran-wage-a-cyberwar-on-the-u-s (accessed on 10th August 2012)

190 Tony Capaccio, Roxana Tiron, *North Korea's cyber warfare capability grows, U.S. general says*, (Bloomberg News, 2012), http://www.staradvertiser.com/news/breaking/144695475.html?id=144695475 (accessed on 11th August 2012)

191 Logic bomb is a piece of code, which triggers under predefined conditions (e.g. period of time). The program executes the order afterwards, in this case overcharging the pipeline.

from the Second World War. [192] Other more recent examples are viruses Stuxnet and Flame. The Stuxnet was programmed to "attack" only certain control system manufactured by Siemens, which were known to have been installed in the Iranian nuclear facilities. The Flame was programmed to collect huge amount of data, including recording from the web cameras, screen snapshots, etc. In both cases the U.S. is supposed to take part, but no official confirmation has been made. Another reason for the lack of precedents is the moment of surprise. Cyber attacks have been introduced very recently and their full potential is still not analyzed. It is in the best interest of particular states not to communicate their capabilities and types of attack they are capable to execute, since such proclamations would only warn potential enemies where their cyber security risks are. Therefore for the purpose of this analyses the amount of scored points is based on mutual comparison of assumed offensive potential of every state, taking into consideration not only objective facts and statistics, but also subjective analytical assessment.

From the perspective of the offensive capabilities the order of analyzed states is as follows from the strongest: U.S., China, Russia, Iran, and North Korea. The strongest countries are U.S., China and Russia, given their officially declared specialized units and recent cyber incidents where is a strong indication that the government was somehow involved. The leading position of the U.S. is thanks to the clear organization of military units and also to the fact that if the cyber plans are openly presented, there is higher probability that secret development will be even more advanced than in the case when only the existence of such specialized units is a secret. The position of the U.S. is also strengthened by the fact that global leading companies in the ICT domain are based in the U.S. Therefore the American army and responsible agencies have access to important know how and also get otherwise classified information, as discussed in the case of PRISM. The second and third positions are very close. Both China and Russia have dedicated units and they are also able to summon groups of hackers if needed. Chinese second position is also based on the fact that vast majority of computer and network hardware is manufactured in China; therefore Chinese units have unique knowledge of the technology. Considering the situation of North Korean army, it is highly probable

[192] Kim Zetter, *Future of Cyber Security: What Are the Rules of Engagement?,* (WIRED, 2009), http://www.wired.com/dualperspectives/article/news/2009/07/dp_security_ars0728 (accessed on 10th August 2012)

that the number of specially trained units will be lower than in Iran, also due to the Iranian experience with Stuxnet.

Mentioned facts projected on the point scale from one to ten in order to allow mutual comparison, the results similar to the score given by Richard A. Clarke.

Country	Points	Points according to R.A.Clark
U.S.	9	8
Russia	7	7
China	8	5
Iran	5	4
North Korea	3	2

The only difference in the score is on the second and third place. The difference may be caused by the recent cyber security issues attributed to China.

10.3. Cyber defense

Defense potential mean the ability to face cyber attacks and proactively minimize their impact. Defense forces are forces dedicated to defend cyber space of the U.S. For the purpose of this paper other factors related to cyber defense and to potential impacts of attack will be disregarded, for instance time needed to restore operation, backup systems, emergency plans, etc. Given the fact that cyber space is the discussed domain, the ability of the U.S. to respond to cyber attacks by kinetic weapons is not considered.[193] Proactive cyber defense itself is very complicated. It is necessary to take into consideration the element of time needed for dangerous attack to take place. Countermeasures or defensive actions have to be executed in seconds after the attack is detected. Moreover, the detection of an attack is a serious question itself. The speed of cyber attacks forces complete reconsideration of current processes. Possible attack by intercontinental ballistic missiles manufactured during the Cold War can be detected shortly after the missiles have been launched. Before the missiles reach the U.S. air space, defense forces have approximately 30 minutes to analyze the problem and take necessary actions to prevent the damage. 30 minutes might seem like a rather short

[193] Potential response by kinetic weapons might be aimed also against targets related to cyber capacity of the enemy, for instance server farms.

period, but compared to cyber space it is ages. Cyber attacks can be executed and directed in the real time leaving practically no space for the analysis of the problem. The defense of cyber space will essentially rely on automated procedures and on emergency scenarios, as there is no time for analysis. Unfortunately, attackers are well aware of this approach and my abuse the emergency procedures to their benefits.

It was already mentioned that the detection of the attack is much more complicated in cyber space than in the real world. The possibility to detect a cyber attack significantly depends on the intentions of the attacker and on the used type of attack. If the attacker wants to use "brutal force" attack, like DDoS, the attack is discovered immediately when it occurs. More sophisticated attacks like viruses or other malware might be very difficult to discover, since the consequences of the attack might become visible long after the attack took place. This counts especially for logical bombs, which can be triggered when specified conditions are met years after the alteration of the software. Attacks aimed at stealing critical data or gaining unauthorized access is also difficult to spot, if executed properly. Obviously because nothing is missing in the case of stealing data. Only indirect evidences might point to the fact that some intruder used the system to copy and transfer critical data. The detection of an intruder or attacker relies mainly on the online analysis of users behavior (in systems) and on the data and communication flows (in the Internet or intranet). System operators and special software are analyzing the behavior and communication in the real time to discover any abnormalities that would suggest that an attack is taking place. The ability to share information between all sectors is critical to discover a cyber attack and knowing about the attack is the first step to effectively defend cyber space.

The knowledge of the attacker is another critical aspect of an effective defense. However, the identity of the attacker is very difficult to discover in cyber space. The investigation of the attacker's identity very often requires international cooperation. The attacker will usually try to hide his IP address and will direct the communication from his computer via several serves located in different countries. Unfortunately, some countries are more reluctant to provide assistance in such investigations. Sometimes the reason is that they do not have necessary means (legal or material) to execute such investigation. In some cases the lack of motivation to cooperate on such investigations is the most important

reason. Nevertheless, even if the international cooperation is fruitful, the result would be the IP address of the computer attacker uses; it will not be the identity of the attacker. This aspect of cyber space is very dangerous in the combination with declared readiness of the U.S. to respond to cyber attacks with kinetic weapons.[194] The attacker might abuse the attribution effect and try to provoke international conflict.

The terrorism is a kind of asymmetrical warfare. The attacker might choose the weakest point in the defense and focus his actions on this target, whether the defender have to secure the whole critical infrastructure. This asymmetry is multiplied in cyber space, because the critical infrastructure sometimes belongs to the private sector. In such cases the defense forces have only limited control over such infrastructure and the can influence the security indirectly by standards and policies.

Because of all stated reasons, the defense of cyber space relies on the implementation of dynamic programs and procedures monitoring the traffic in the network and in particular systems. They search for suspicious behavior and abnormalities, which can be a proof of ongoing cyber attack. Based on prepared scenarios, the suspicious communication or user will be tracked or possibly logged off the system, depending on the severity of his behavior and on the program. Specialized analysts form another important layer of cyber defense. They are responsible for the analysis of more complex problems and they decide, whether serious attack is taking place or it is just an anomaly in the data.

10.3.1. Defense forces of the U.S.

The importance and formulation of national cyber defense in the U.S. is reflected in the activities of particular commissions and their reports. Another level is represented by the national cyber defense policy and strategy. One among the first commission, which took into consideration the cyber dimension when analyzing the safety of critical infrastructure, was the commission set up by president Clinton in 1997, the Presidential Commission on Critical Infrastructure Protection. Topics raised by this commission were

[194] For instance a notice in Department of Defense report for Congress from 2011, Department of Defense, *Cyberspace, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011,* (Department of Defense, 2011), Section 934, http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf (accessed on 11th August 2012)

further analyzed and resulted in the formulation of National Plan for Information System Protection in 2000. National Strategy to Secure Cyber Space, signed by President Bush in 2003 and Comprehensive National Cyber Security Initiative established in 2008 are two other major activities on the field of cyber defense and cyber security in the U.S. Unfortunately, the implementation of particular measures and recommendations have not reached sufficient level to significantly improve the cyber defense of the American cyber space and to lower the risk of cyber attack.[195]

Despite the size and organization of military units responsible for the execution of offensive actions, the cyber defense of the U.S. is rather weak. Particular units of the American army are responsible also for the protection of military networks and critical military systems. Other networks and systems of the Federal government are defended by the Department of Homeland Security. However, the defense of the private sector or important infrastructure in private hands is not addressed by governmental policies. Alarming is also the fact that some systems ranked as a critical infrastructure systems (e.g. distribution of electricity systems) is managed by private companies (according to some sources almost 85% of infrastructure).[196]

10.3.2. International comparison

There is practically no relevant information about defensive forces considering other countries, nor any information about the structure of cyber defense. The basis for this analysis is therefore deducted from the offensive potential, since offensive capacities can be used also for the defense, even if with reduced efficiency. Nevertheless it is necessary to take into consideration other factors as well before setting the score.

One of the important factors influencing the level of cyber defense is the control over the connection to the Internet. If the connection is provided directly by private companies and not through a state organization in cooperation with private subjects, there is only indirect control of the connection to the internet. Therefore immediate "switching off"

---

195 Richard A. Clarke a Robert K. Knake, *Cyber War,* (HarperCollins: New York, 2010), chapter The Defense Fails. Author presents an example of a new institution without necessary authority.

196 William Mcborrough, *The Need for Improved Critical Infrastructure Protection,* (infosec island, 2012), http://www.infosecisland.com/blogview/21616-The-Need-for-Improved-Critical-Infrastructure-Protection.html (accessed on 15th September 2012)

the Internet would not be so easy. This option might be important in case of massive cyber attack when disconnecting ordinary users would allow to use available resources for the defense or simply to stop the spreading of malicious software. In case of China and North Korea, the connection to the Internet is under the control of the state. Iranian approach is more influenced by more liberal systems; nevertheless the role of the state is still very strong. The highest number of Internet connection providers is without doubt in the U.S., in our sample followed by Russia.

Another important factor is the size of the target. The more systems are used in the country, the higher the number of potential targets defense forces have to protect. Even when considering only public administration networks or critical infrastructure systems, the advantage of "less networked" countries is visible. There are only few systems in North Korea, which can be regarded as critical for the state. Therefore the defense can be focused easily on those systems. If critical infrastructure in private hands is also included, the supremacy of North Korea in this category remains unchanged. Second in the lowest number of possible targets is Iran followed by Russia. There are the highest numbers of possible targets in the U.S. with significant lead over Russia.

Projecting discussed aspect into points leads to following results:

Country	Points for offensive potential	Points for access to Internet control	Points for number of targets	Final score	Score according to R.A.Clarke
U.S.	3	0	0	3	1
Russia	1	1	0	2	4
China	2	2	1	5	6
Iran	0	1	2	3	3
North Korea	0	3	3	6	7

Final scores show that R.A.Clarke's results are even more pessimistic for the U.S. The differences in score are mainly due to the points for offensive potential. This factor might have not been included in the original analysis. Nevertheless, it is possible to say that the results in consider recent changes in the U.S. security policy towards the Internet resulting into higher level of control.

10.4. Dependency on cyber space

The dependency on cyber space is the result of increasing usage of ICTs, computers and cyber space in the public and private sectors. Nevertheless, increased usage does not cause the dependency, but it is the prerequisite condition for dependency to exist. Dangerous dependency is caused mainly by the absence of business continuity plans, emergency scenarios and alternative solutions or workarounds; for example submitting a tax return as an example. Submitting the tax return online is on the rise in the Western countries. When the ratio of tax returns submitted online significantly exceeds other ways of submitting the tax return, it might be declared to be the only allowed way how to submit the tax return. It makes sense since vast majority of people uses this way and it is significantly cheaper in terms of related costs. During following years the transition of submitting tax returns will be complete. Alternative scenarios will be prepared in the first years, for instance reopening relevant offices. But after some more years, it is highly probable that alternative procedure will not be updated, necessary equipment will not be sufficient and no workaround will be available. At this moment dangerous dependency emerges. In case of system failure when no alternative solution is ready and the system recovery might take weeks, such dependency might cause significant damage.

Increasing usage of ICTs and economic motivation to reduce costs disregarding potential risks can create dangerous dependencies, which can be exploited by terrorists. In other words, the dependency on cyber space can expressed as the amount of damage caused by successful attack exploiting this dependency. The higher is the damage, the higher is the dependency on cyber space.

10.4.1. Dependency on cyber space in public sector

Public sector has been recently forced to pay more attention on the efficiency and on the cost reduction due to difficult economic situation. However, there are other factors in public sectors, security of the state, for instance. Some solutions might not be very effective, but they are more secure. For example, president of the U.S. cannot travel together with vice-president on the same plane. Of course that it is not efficient, but it is more secure. Despite the fact that the probability of successful attack on the Air Force One is very low, potential consequences of such attack is so high that there is no space

for cost reduction or efficiency. Let's assume that similar approach will be used for critical federal and national systems. It is possible to expect that the federal backbone network will be immediately replaced or restored in case of failure. Again, potential damage caused by this failure is so significant that security is more important than cost reduction. Current pressures on the cost reduction in public sector therefore do not necessarily cause the increase of dangerous dependency, provided that all critical infrastructure and all its components are identified and duly secured.

10.4.2. Dependency on cyber space in private sector

The dependency on cyber space in private sector is the consequence of strategy aimed at reducing costs and increasing profits. Implementing more efficient solutions including modern ICTs is the main tool for this kind of strategy. Modern systems for information analysis, effective resource management and planning, supply chain management and many others enables companies to gain competitive advantage. Benefits of the implementation of new ICTs are easily calculated and they are significant. However, costs related to creating secure solutions are also very high while the benefits of highly secure solution are visible only in case of an attack or serious incident. Complex security of ICTs in a company would probably consume all resources saved by the implementation of ICTs. Therefore implemented security measures are based on the effectiveness. Sometimes it is cheaper to be insured than to implement particular costly security measure. Business continuity plans in some companies therefore take into consideration needed time to purchase new hardware and software. In some cases it is more efficient to stop the business for certain period than to have backup system. Of course, companies in certain sectors are obliged by the law or regulatory authority to have specified level of system security. But again, the main task of a company is to make profit and create value for the shareholders. Let's consider data warehouse in a bank for an example. Using cost and benefit analysis, the bank arrived to a conclusion that it is more efficient to wait two months in case of catastrophic event for new equipment to be installed rather than to have parallel backup system. It is also important to be aware of the fact that the presence of backup data or backup solution does not necessarily mean better security.[197] Moreover, the system restoration is so complicated and time

[197] The installation of system takes some time. Afterwards, it is necessary to specify at what time the incident occurred and select appropriate data from the backup. The migration to the new or repaired

consuming that it is seldom tested. Therefore many companies rely on the theoretical procedure how to restore the system without ever testing it.

It is important to say that companies will not commence to enhance their cyber security from their own initiative. They may be forced by changes in the regulation, by shift of market standard or by higher probability of security incident which means also higher probability of economic loss. In other words companies will improve their level of cyber security only if they are obliged to do by the law or by the market.

10.4.3. Dangerous dependency on cyber space

Dangerous dependency appears when there is no alternative solution and the system or ICT is the only option. In such case any attack able to disable the service or disrupt the system might cause significant damage, because there is no other way how to restore the system or service. This is likely to happen especially in quickly changing environment, where security standards become obsolete in short periods of time, sometimes even before they are successfully implemented. Cyber space is such quickly changing environment and rigorous standards may in time create dangerous dependency, since new types of attack would make the security standards and emergency scenarios useless. Another important factor is the definition of critical infrastructure. It might happen that the usage of ICT might cause that the system or ICT itself becomes part of critical infrastructure. ICT might be the weakest point in the defense of critical infrastructure, if not well protected. Server farms, collectors, optic cables can be regarded as a critical infrastructure, because 'standard' critical infrastructure might depend on them. Hence it is important that the critical infrastructure definition is wide enough to cover also the cyber dimension. Critical infrastructure therefore might be in the private hands. Corporate sector might own and operate networks or ICT solutions, which can be regarded as a critical infrastructure. Or the service and operation might be outsourced to private company. Despite the fact that public sector can afford certain level of ineffectiveness in exchange for higher security, there is a strong pressure on significant costs reduction, as discussed before.

---

system is also very complicated and time consuming. After the migration of data, time consistency errors may occur in the data and it is necessary to repeat the whole procedure.

There lies a critical role in the creation of security standards for national administration – to ensure sufficient level of cyber security both for outsourced solutions or services and for those in possession of private companies. Security standards and control are the only way for public administrations to ensure the cyber security. However, because of the dynamic evolution of cyber space and modern technologies, the security standards might become obsolete, thus creating a security risks or dangerous dependency.

10.4.4. International comparison

There are no doubts that the country with lowest dependency on cyber space is the North Korea. Not only the usage of cyber space is significantly lower, than in other cases, but also the dependency of private sector is not important thank to the low usage of ICTs and other modern technologies. And even if the few systems were attacked, manual workarounds would be easily introduced. On the other hand the dependency on cyber space in the U.S. is significantly higher than in China, Russia and Iran. This is partially due to the fact that all major ICT companies are based in the U.S. and that the amount of electronic transaction is significantly higher than in other countries. Some companies are completely dependent on cyber space (Amazon, eBay and others) and any major issue might hamper their business. Also the level of implementation of modern ICTs into the critical infrastructure is higher than in other countries mentioned in this analysis.

The comparison among remaining countries in the middle of the list is more difficult. Based on the low number of Internet users it is possible to deduce that the dependency on cyber space is lower in Iran than in China and Russia, despite the Stuxnet attack. Taking into consideration the level of cyber space control in China and Russia, the dependency is lower in China since the Chinese government has more efficient control over the Chinese cyber space then Russia. Also the possibility to efficiently implement emergency workarounds is slightly higher in China thanks to recent rapid development of ICT industry in China. Chinese position in the comparison with Russia is also supported by the fact that vast majority of ICT hardware is manufactured in China.

Given all the facts and differences among particular countries, the score is as follows.

Country	Points	Points according to R.A.Clarke
U.S.	2	2
Russia	5	5
China	6	4
Iran	7	5
North Korea	9	9

The differences are rather small and do not influence the interesting fact that the U.S. came last in this comparison.

10.5. Conclusion

Cyber space is a completely new domain, which can be used, abused and conquered. Current tactics used in the army based on the former experience are inefficient and the progress in research is slower that the evolution of cyber space. The ability to execute efficient cyber attack might be the decision point in modern conflicts. The number of cyber attacks will likely increase as well as their complexity. The main reason is the fact that rapid implementation of ICTs in private and public sector creates dangerous dependencies. Cyber space thus offers a possibility to efficiently attack the adversary without being revealed. It is true that the probability of successful major cyber attack is decreasing due to the introduction of cyber security measures, but in combination with low probability of attacker's identification the cyber attacks are still a very tempting option. The U.S. and other states are well aware of this situation and they are introducing relevant policies and standards. However, the impact on the level of cyber security is lower than expected as displays following chart showing the scores in key aspects:

Country	Offensive capabilities	Defensive capabilities	Dangerous dependency	Total score	Total score according to R.A.Clarke
U.S.	9	3	2	14	11
Russia	7	2	5	14	16
China	8	5	6	19	15
Iran	5	3	7	15	12
North Korea	3	6	9	18	18

Total score represents the overall strength of given country in cyber space based on aspects analyzed in this part. It is important to point out that the points serve mainly to illustrate relative position of particular country in comparison to other countries in the sample. Therefore the final rank of countries is much more relevant than concrete points.

Final results based on three aspects shows that despite the strength of the American army on "conventional" fields and their offensive cyber capabilities, the overall position in cyber space is not so good. It is not important how many points the U.S. lacks from other states and in which aspects, but the fact that other global powers like China and Russia have better results. Surprisingly even North Korea, otherwise on completely different level of military strength might use the opportunity to cause significant damage to the U.S. using their cyber space potential in combination with high level of cyber dependence in the U.S. The results reject the initial hypothesis that the U.S. have a superior position in the cyber space. It is obvious that the main goal of American government is to improve the level of cyber security in the U.S. and reduce the dangerous dependency on the ICTs and on cyber space.

The offensive potential of the U.S. in cyber space is still significant and probably more advanced than in other countries. Nevertheless, the high level of dependency and ambiguous approach towards the cyber defense of critical infrastructure systems make the U.S. vulnerable mainly in the asymmetrical conflicts when attackers focus on the weakest point in the defense to cause maximal damage. If such attack occurred, very

strong standards and regulation would presumably have been introduced. But such measures currently lack political support to be introduced. Another important fact is that the superiority in the offensive cyber capabilities is not relevant in all cases. For instance it is impossible to fully benefit from this offensive potential in Iraq or Afghanistan, because the number of potential targets is very low. On the other hand, skilled cyber terrorist might choose only one from the abundance of possible targets in the U.S. to cause significant damage.

Following facts are some of the principles valid in cyber space, which also influence the final scores of particular countries:

- Preventive attack in cyber space will not protect national assets since it is impossible to significantly reduce opponent's cyber offensive capabilities by a cyber attack.
- The vulnerability to cyber attacks is caused by the level of ICT usage in the critical infrastructure without existing possibilities to immediately replace critical hardware or to introduce emergency workarounds.
- The definition of critical infrastructure might be different in cyber space and sometimes is completely out of state control.
- Consequences of successful cyber attack are immediate. There is only limited time to analyze the problem and to find optimal solution. The basis of efficient reaction is therefore detailed emergency scenarios and plans.
- The identification of the perpetrator is almost impossible without international cooperation and it is time consuming.
- Possible cyber conflicts are asymmetrical, thus very interesting for terrorists or states avoiding direct confrontation.
- The dominance in cyber space might reduce the technological advantage of the army due to the high level of usage of modern technologies and ICTs in the army.

11. American security policy

11.1. Introduction

The aim of this chapter is to analyze documents shaping American security policy and track possible influence of cyber terrorism. But since previous chapters stated, cyber terrorism is only one possible threat present in cyber space. It is therefore necessary to include in the analysis the cyber security, as documents addressing cyber security in general might be related to cyber terrorism as well. This chapter will also analyze the evolution of cyber space as a topic in relevant documents. The reason is that the importance of cyber space and cyber security has been increasing in last 30 years, but it was influenced by other topics important in that time. The hypothesis for this chapter is that documents influencing American security policy do not address directly the threat of cyber terrorism and therefore the threat of cyber terrorism does not have direct influence on American security policy.

11.2. Methodology

Documents selected for further analysis were firstly chosen based on the author's knowledge. The list of documents was then compared with three other overviews of such documents with similar topic. The first one is the overview of policies related to critical infrastructure protection.[198] The reason for using this document is the fact that protection of critical infrastructure was the first domain recognizing the importance of cyber security (see documents below). The second list of relevant documents is the timeline of US Government and cyber security.[199] This timeline provides very detailed overview of documents recognized as important by the press. The third overview is the report of a recognized consultant agency.[200] The fourth overview is the timeline of US

[198] John D. Moteff, *Critical Infrastructures: Background, Policy, and Implementation*,(Congressional Research Service, 2014), http://fas.org/sgp/crs/homesec/RL30153.pdf (accessed on 21st September 2014)

[199] Washingtonpost, *Timeline: U.S.Government and Cyber Security,* (washingtonpost.com, 2003), http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html (accessed on 19th September 2014)

[200] Booz, Allen, Hamilton, *Milestones of Cyber Security,* (Booz, Allen, Hamilton, 2009), http://www.boozallen.com/media/file/milestones-of-cyber-security.pdf (accessed on 1st September 2014)

cyber security policy in context.[201] The initial list of documents was validated against mentioned four other sources. The final list therefore contained only documents mentioned at least in one of the overview. There are several reasons for using four different overviews to identify the most appropriate documents. Firstly, the overview do not use the same time period for documents analysis. Having more overviews allows expanding the period for analysis, but in general to focus was on years from 1995 to 2013. Secondly, the overviews were created by different authors for different purposes. The overviews therefore take different point of view and the combined list is wider then if all the overview were created with regard to critical infrastructure, for instance. The overviews were created by state authority, journalists and private sector consultants.

Documents analyzed in this chapter include bills, draft of bills, strategies, policies, executive orders and other legislative documents. Reports of incidents, newspaper articles and other documents without direct influence on the American security policy were not analyzed. In some cases the document is analyzed despite the fact that it was not put in practice or enacted. 23 documents in total were analyzed covering the period from 1977 till 2013. The selection of the documents is not extensive. There is no document analyzed for some years due to the fact that either no document with significant influence on the security policy in relation to cyber security was identified, or the document does not contain any new aspects important for the purpose of this chapter. On the other hand, there are many documents issued in the last years due to the increased importance of cyber security, but only few are analyzed in this chapter.

First the content of selected documents is analyzed. This content analysis is applied to provide the essential thoughts of analyzed documents from the perspective of cyber security and cyber terrorism. The document is also analyzed on the syntactic/semantic level in relation to the communicator. The communicator is a governmental body in majority of analyzed documents. First step of analysis focuses on the usage of the term "cyber terrorism." Usage of this exact term in the content part of the document confirms that the document acknowledges the possibility of terrorists executing a cyber attack and this possibility is reflected as a threat. Second step searches the text for the content

[201] Andrea Peterson, Sean Pool, *Timeline: U.S. Cyber Security Policy in Context,* (Science Progress, 2013), http://scienceprogress.org/2013/02/u-s-cybersecurity-policy-in-context/ (accessed on 2nd September 2014)

related to cyber attacks and terrorists. Despite not using the term "cyber terrorism," the document might reflect the possibility of terrorists launching a cyber attacks. But in this case the document focuses on different subject as the terrorists are only one possible source of cyber attacks. Third step of the analysis focuses on the cyber attacks. Cyber attacks might be related to criminal, viruses, states, but also to individuals and non-state groups. Given the fact that terrorists can be regarded as a non-state group and in some cases also as individuals, the document in its sense might consider terrorists as possible source of cyber attacks. Fourth step of the analysis focuses on the context meaning of cyber security. The term itself does not have to be used, but the documents will address some of the issues related to the cyber security. The way, in which this topic is addressed, defines the approach to the cyber security in this document. This step will focus particularly on the separation of cyber security from related topics such as critical infrastructure protection.

11.3. Analyzed documents

11.3.1. Federal Computer Systems Protection Act[202]

Federal Computer Systems Protection Act was introduced in the Congress in 1977 by Senator Abraham Ribicoff. It was modified in following years and repeatedly discussed, but the Congress had not taken any decisive action based on this document.

This Act is one of the first documents actually dealing with the problem currently described as cyber security. It states that the usage of computers is growing and therefore the usage of computers is actually necessary to provide basic governmental services. However, controls and checks existing in the physical world are sometimes not applied neither sufficiently substituted for. Such situation leads to security incidents, when computer crimes occur causing significant financial damage. It gives several examples of incidents that actually occurred in the United States to demonstrate the risk.

[202] *S.1766 – Federal Computer Systems Protection Act,* (Washington, Congress, 1977), http://www.gao.gov/assets/100/98793.pdf (accessed 27th October 2014)

The Act actually defines computer crimes related to:

- the introduction of fraudulent records or data into a computer system;
- the unauthorized use of computer-related facilities;
- the alteration or destruction of information or records;
- the stealing, whether by electronic means or otherwise, of money, financial instruments, property, services, or valuable data.

It makes a Federal crime to actually access a computer system in connection with Federal agency, financial institution or affecting commerce, for fraudulent purpose.

The term "cyber terrorism" is not used in this document. Nevertheless, the introduction to this document mentions several cases of supposed sabotage. The document was supposed to define cyber crimes punishable on Federal level. This can be regarded as an attempt to create legislator conditions to actually improve the cyber security.

11.3.2. Computer Security Act of 1987[203]

Computer Security Act was introduced in 1987. It focuses mainly on the development of acceptable security practices and standards within the Federal computer systems dealing with non-classified information. The Act actually changes the responsibilities as defined in National Security Decision Directive 145 issued by President Reagan, which gave all the control over governmental information to NSA.

It gives the responsibility for developing standards and guidelines for Federal computer systems to the National Bureau of Standards (National Institute for Standards and Technology - NIST), when dealing with non-military or unclassified data. These standards and guidelines are supposed to enable cost-efficient security and privacy of sensitive information in Federal networks and prevent fraud and misuse of such information. The NIST is to be responsible for the necessary training, validation procedures and other activities described in the document.

[203] *H.R. 145: Computer Security Act of 1987,* (Washington, Congress, 1987), https://epic.org/crypto/csa/csa.html (accessed on 16th September 2014)

This document only changes the responsibility regarding the protection of Federal networks. It does not use the term "cyber terrorism"; neither it mentions the risk of cyber crime. The actual risk described in this document is the misuse or leak of sensitive, but unclassified, non-military information. On the other hand it highlights the necessity to increase security (cyber security) of Federal networks and names important processes, which when implemented by NIST will improve the cyber security of Federal networks.

11.3.3. Computer Network Protection Act of 1989[204]

Computer Network Protection Act of 1989 was introduced by Edward Markey. The aim of this act was to discourage creation and distribution of computer viruses and also to criminalize computer criminal activities. The act was not brought to a vote.

The Act acknowledges the importance of computers and network communication for the United States. It specifically mentions its strategic importance, influence on business and research potential. It stresses the danger of computer attacks leading to loss of data, misuse of data and in general to financial loss. It defines the procedure how to prosecute the perpetrators with regards to a very strong statement that "there is no technological defense capable of deterring computer virus attacks."[205]

The document does not use the term "cyber terrorism," neither if refers to cyber security. It mainly focuses on the criminalization of activities possibly leading to creation and distribution of computer viruses; or to activities possibly described as cyber crime. The main purpose is to deter the possible perpetrators, not to increase the cyber security as per se. The absence of cyber security dimension can be related to a very interesting statement stated above – there is no defense against computer viruses. Therefore the only option is to deter possible perpetrators.

11.3.4. Communications Assistance for Law Enforcement Act[206]

[204] *H.R.3524: Computer Network Protection Act of 1989,* (Washington, Congress, 1989), http://thomas.loc.gov/cgi-bin/query/z?c101:H.R.3524.IH: (accessed on 16th September 2014)
[205] Ibid, page 2, section 2, article 4
[206] *H.R.4922: Communications Assitance for Law Enforcement Act,* (Washington, Congress, 1994), http://www.gpo.gov/fdsys/pkg/BILLS-103hr4922rds/pdf/BILLS-103hr4922rds.pdf (accessed on 15th September 2014)

Communication Assistance for Law Enforcement Act (CALEA) was introduced in 1994 during President Clinton administration. The main purpose of this bill was to provide law enforcement agencies with options how to perform surveillance of electronic communication, provided a court order or other legal authorization was presented. It actually forced telecommunication companies to modify their equipment in a way that enabled storage of information defined in the bill. The goal of this bill was to react to the development and increase usage of digital telephone exchange switches. Nevertheless, the CALEA have been actually expanded to cover VoIP and broadband traffic surveillance as well.

The bill itself focuses on precise definition of subjects regulated by this bill and on the detailed description of requirements. It of course mentions technical standards and the possibility of financial compensation of costs related to this regulation (under specific conditions).

The CALEA does not uses the term "cyber terrorism," neither it mentions security of networks in the sense used in this document (it mentions the security of the stored information in the sense of access management). The document formulates the requirements and sets the procedures, but it does not refer to the cyber security. Its aim is to provide the legal enforcing agencies with the possibility to actually access communication data, when requested. Therefore the CALEA itself has not influenced the level of cyber security, but it provides legal enforcing agencies with a powerful source of information for their investigations of criminal and other illegal activities.

11.3.5. Executive Order 13010 – Critical Infrastructure Protection[207]

Executive Order 13010 was issued in 1996 by President Clinton and it established the President's Commission on Critical Infrastructure Protection.

The executive order defines the members of the Commission as well as the process how the President shall be informed about its activities and results. It establishes other bodies (Principals Committee, Steering Committee, Advisory Committee) as well. The

[207] William J. Clinton, *Executive Order 13010 – Critical Infrastructure Protection,* (Washington, White House, 1996), http://fas.org/irp/offdocs/eo13010.htm (accessed 14th September 2014)

mission of the Commission is to identify and consult stakeholders in critical infrastructure protection both from private and public sector, asses the threats and vulnerabilities in relation to the critical infrastructure, determine legal issues related to critical infrastructure protection, recommend a national policy and implementation strategy to ensure critical infrastructure protection addressing all identified threats and vulnerabilities, propose organizational changes and to report on its activities. The initial mission of the newly established Commission is to elaborate on these points and present detailed mission statement.

This executive order focuses on critical infrastructure protection. Despite the fact the document does not employ the term cyber terrorism; it stresses the cyber threats that exists along the conventional physical threats to national critical infrastructure. Cyber threats in this document are defined as "…electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures."[208] Nevertheless, the document does not define possible attackers executing such attacks, therefore it does not explicitly states that terrorists could take this opportunity and execute a cyber attack against the critical infrastructure.

Despite the fact that this executive order establishes a body to assess the existing threat and to plan actions aimed at increasing the security of critical infrastructure, it is not aimed only on the cyber security, but on the security of critical infrastructure in general.

11.3.6. Presidential Decision Directive 62[209]

Presidential Decision Directive 62 was issued by President Clinton in 1998. It reacts to the increasing security risk of terrorist attacks against United States, possibly targeting the critical infrastructure. This directive in general introduces more systematic approach to the terrorist threat on national level and initiates deeper international cooperation of counter-terrorism activities.

[208] William J. Clinton, *Executive Order 13010 – Critical Infrastructure Protection,* (Washington, White House, 1996), http://fas.org/irp/offdocs/eo13010.htm (accessed 14th September 2014), page 1 - Introduction

[209] William J. Clinton, *Presidential Decision Directive 62,* (Washington, White House, 1998), http://fas.org/irp/offdocs/pdd/pdd-62.pdf (accessed 14th September 2014)

Despite the success on the field of critical infrastructure protection, this directive introduces a new integrated program to address the remaining challenges. The overall program was to be coordinated by newly created position – the National Coordinator for Security, Infrastructure Protection and Counter-terrorism. The overall program consist of following issues:

1. Apprehension, Extradition, Rendition and Prosecution
2. Disruption
3. International Cooperation
4. Preventing Terrorist Acquisition of Weapons of Mass Destruction
5. Consequence Management for Terrorist Incidents
6. Transportation Security
7. Protection of Critical Infrastructure and Cyber Systems
8. Continuity of Government Operations
9. Countering the Foreign Terrorist Threat in the U.S.
10. Protection of Americans Overseas

The document does not use the term "cyber terrorism" to define a possible threat, but it does mention the possibility of states or state sponsored groups engaging in cyber warfare. Unfortunately, the document does not give the definition of cyber warfare. It states that information and computer-based technologies are vulnerable to a terrorist attack. The program for Protection of Critical Infrastructure and Cyber Systems declares the possibility that individuals, groups or nations may attack the cyber systems. Despite the fact that the document does not explicitly relate possible cyber attacks to terrorist, it is very probable that the possibility of cyber terrorism is included in this directive. One of the reasons why the possibility of terrorist committing cyber attacks is not explicitly mentioned[210] might be the prevailing thought that terrorists will seek to acquire weapons of mass destruction. This opinion was supported by the attacks in Tokyo.

[210] The threat of terrorist engaging in cyber warfare is actually mentioned in the electronic version of unclassified abstract of the Presidential Decision Directive 62 (http://fas.org/irp/offdocs/pdd-62.htm). However, in the original scanned document (http://fas.org/irp/offdocs/pdd/pdd-62.pdf), the term terrorist groups is not used. It uses states and state sponsored groups instead. This discrepancy might be caused by the fact that the electronic version was updated in 2014.

The cyber security itself is covered under the point Protection of Critical Infrastructure and Cyber Systems, but it is elaborated more deeply in a different document (see below). This document focuses on the terrorist threat and critical infrastructure protection. It indeed acknowledges the threat of cyber attacks (cyber warfare) and it also admits that such attacks might be committed by individuals or groups.

11.3.7. Presidential Decision Directive 63[211]

Presidential Decision Directive 63 was issued by President Clinton in 1998 together with Presidential Decision Directive 62, where it is referenced in the part number 7 – Protection of Critical Infrastructure and Cyber System.

The document states very important fact that America's military and economic strengths are "increasingly reliant upon certain critical infrastructures and upon cyber-based information systems. (…) As a result of advances in information technology and the necessity of improved efficiency, however these infrastructures have become increasingly automated and interlinked. (…) Because our economy is increasingly reliant upon interdependent and cyber-supported infrastructures, non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy."[212]

Despite the fact that the directive focuses on the critical infrastructure, the cyber aspects has more attention compared to previously issued documents. Newly emerged vulnerabilities can become targets for nations, group or individuals attempting to cause damage but avoiding traditional direct and open conflict. The document elaborates on the introduced organizational changes in order to coordinate the effort to prevent attacks on critical infrastructure and cyber system and to develop efficient framework to minimize possible damage. Since some of the critical infrastructure and cyber systems vital to the country are in private ownership, deeper cooperation with private sector is necessary. Public-private partnership is mentioned as one on the key goals for the near future to increase the level of security. Since the critical infrastructure and cyber systems are spread among different industries, each infrastructure sector shall be

[211] William J. Clinton, *Presidential Decision Directive 63,* (Washington, White House, 1998), http://fas.org/irp/offdocs/pdd/pdd-63.html (accessed 14th September 2014)
[212] Ibid, page 1, part 1 – A Growing Potential Vulnerability

managed by a single U.S. Government departments responsible also for cooperation with private sector. Special sectors on federal level will be addressed by designated agencies. Major role is assigned to Federal Bureau of Investigations (FBI), which will serve as a full scale National Infrastructure Protection Center. The interagency coordination will be ensured under the auspices of a Critical Infrastructure Coordination Group, chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. National Coordinator will be appointed by President and will report to him. Moreover, major infrastructure providers and selected officials will form President's National Infrastructure Assurances Council[213] to strengthen public private partnership.

This document does not use the term "cyber terrorism," but it states that nations, groups or individual might attack critical infrastructure or cyber systems. The motivation of the attackers is not distinguished in the directive. It focuses on the vulnerabilities and risks, not on the motivation of attackers. The term terrorism is used only once in the whole document. Even if the document recognizes the vulnerabilities related to cyber systems, the cyber security itself has not become an independent topic. Cyber security is still an aspect of critical infrastructure protection. Nevertheless, this directive attempts to coordinates the efforts to monitor and increase cyber security in different industries and sectors. The directive creates conditions and framework to increase the cyber security level.

11.3.8. National Plan for Information Systems Protection[214]

National Plan for Information Systems Protection was issued by President Clinton in 2000 and it continues in the direction described in Presidential Decision Directive 62 and 63. This plan describes major milestones in the process to reduce the vulnerability caused by increased usage of information technology in the critical infrastructure and by the emerging reliance such systems.

---

[213] National Infrastracture Assurance Council was created by President's Executive Order 13130 issued in 1999.

[214] President's Office, *National Plan for Infromation Systems Protection,* (Washnigton, White House, 2000), http://clinton4.nara.gov/media/pdf/npisp-execsummary-)00105.pdf?bcsi_scan_26e330b4cc75177f=0&bcsi_scan_filename=npisp-execsummary-000105.pdf (accessed on 18th September 2014)

National Coordinator, Richard A. Clark, affirms in the introduction to this document that United States is dependent on its cyber space more than any other nation. Therefore the national plan is of high importance as it is the first attempt by a national government to design a way how to protect its national cyber space. The document itself introduces 10 programs aimed at particular issues related to cyber security and cyber defense ranging from identification of critical assets to increased funding of research related to cyber space. These programs are divided into three groups titled Prepare and Prevent, Detect and Respond, Build Strong Foundation. Apart from introducing these programs, the document also presents an overview of responsibilities and authorities for particular aspects of cyber security.

The term "cyber terrorism" is not used in this document. However, the document clearly states that perpetrators attempting to cause substantial damage may also be terrorist. The document therefore presumes the possibility of terrorists executing a cyber attack. The cyber security is for the first time listed as an independent topic. Despite the fact that the document also stresses the relationship between information systems and critical infrastructure, the cyber defense and cyber assets are stated alongside critical infrastructure. The term cyber security is not used neither in this document. Computer security or system security is used instead. On the other hand, cyber defense term is mentioned as a topic of the nearest focus.

This plan presents concrete programs and actions with appropriate timeframe to increase the cyber security through various programs ranging from increased cooperation with private sector to security standards. This plan also states that efforts to increase the level of cyber security must be compliant with civic liberties.

11.3.9. USA Patriot Act[215]

The USA Patriot Act was signed into law by President Bush in 2001 in reaction to 9/11 terrorist attacks. The document mainly widens the options for security agencies to acquire intelligence on terrorist activities and to better face the terrorist threat. This law has been widely discussed from different aspects mainly because of its alleged violation

[215] *H.R. 3162: USA Patriot Act,* (Washington, Congress, 2001), https://epic.org/privacy/terrorism/hr3162.html (accessed on 16th September 2014)

of personal rights and freedoms granted by the Constitution. Of course that Patriot Act is a cornerstone for counter-terrorist activities in the after 9/11 world, but from the cyber security perspective it is not that important.

However, Patriot Act for the first time uses the term "cyber terrorism." Cyber terrorism is defined as activities that "…caused or would have caused, if completed, loss of at least 5000 USD to one or more persons in one year, or an activity modifying medical documents, causing physical injury to a person, threat to public health or safety, or causing damage or affecting system used by a government entity for action related to justice, national defense or national security."[216]

11.3.10. Executive Order 13228[217]

The Executive Order 13228 was issued by President Bush in 2001. The main purpose of this document is to establish the Office of Homeland Security within the Executive Office of the President. The mission of this new office is to coordinate the implementation of national strategy to prevent terrorist activities. The document therefore describes the pattern for cooperation with particular departments, agencies and other executive offices. The Office of Homeland Security became a cabinet-level department in 2002 when Congress passed the Homeland Security Act in 2002 (see below).

The mission of the Office is clear – coordinate national efforts to fight terrorism. On the level of the establishing executive order the "cyber terrorism" is not mentioned. Nevertheless, the Order states that one of its tasks is to "coordinate efforts to protect critical public and privately owned information systems within the United States from terrorist attack."[218] The document therefore acknowledges the possibility that terrorist might target the information systems. However, it is not clear from the text if the protection should consider also the cyber dimension or focus solely on the physical protection. Information systems are also mentioned in the article f) Response and Recovery, point (ii), where it is stated that the Office shall coordinate necessary efforts

[216] Ibid, Section 814. Deterrence and prevention of cyber terrorism
[217] George W. Bush, *Executive Order 13228,* (Washington, White House, 2001), http://georgewbush-whitehouse.archives.gov/news/releases/2003/01/text/20030124.html (accessed on 21st September 2014)
[218] Ibid, article e) Protection, point (ii)

to restore the systems after attack. Otherwise the cyber security is not concerned in the document.

11.3.11. Executive order 13231[219]

The Executive Order 13231 was issued by President Bush in 2001. It recognizes the importance of information systems security, especially when such systems support critical infrastructure or important government functions or services.

President's Critical Infrastructure Protection Board chaired by the Special Advisor to the President for Cyber Space Security is established by this order. The purpose of the Board is to recommend policies and to coordinate programs for protecting information systems for critical infrastructure. Despite the fact that these activities should be focused on public sector, the document highlights the necessity to cooperate with private sector. In parallel with this activity, the Director of the Office of Management and Budget (OMB) is given the responsibility to develop and to supervise the implementation of policies, principles, standards and guidelines for the security of information systems supporting the executive branch. National Security Information Systems are set apart from the responsibility of OMB. Security of these information systems is managed by the Secretary of Defense and the Director of Central Intelligence. The document also describes the processes of information sharing and highlights the role of the Office of Homeland Security for these issues. The Order established National Infrastructure Advisory Council, which shall advise the President on the security of information systems for critical infrastructure.

This document does not use the term "cyber terrorism." Possible attacks against information systems are mentioned only with reference to the role of the Office of Homeland Security. The document does not otherwise describe the risks of possible cyber attacks. Nevertheless, the document recognizes the importance of information systems supporting critical infrastructure, governmental functions or important industries. Bodies established by this document have mainly coordination activities; therefore the immediate effect on the level of cyber security was very limited.

---

[219] George W. Bush, *Executive Order 13228,* (Washington, White House, 2001), https://www.dhs.gov/xlibrary/assets/executive-order-13231-dated-2001-10-16-initial.pdf (accessed on 21st September 2014)

11.3.12. National Strategy for Homeland Security[220]

The first National Strategy for Homeland Security was published in 2002 and it was later updated in 2007. This document builds on the analytical work done by the Office of Homeland Security and generally follows in the direction established by preceding executive documents concentrating on the counter terrorism efforts and internal security. The Strategy presents the intention to create new cabinet-level body solely for the homeland security (future Department of Homeland Security). The document describes three main strategic objectives of the homeland security:

- Prevent terrorist attacks within the United States
- Reduce America's vulnerability to terrorism
- Minimize the damage and recover from attacks that do occur

These objectives are in line with the more detailed critical mission areas:

- Intelligence and warning
- Border and transportation security
- Domestic counterterrorism
- Protecting critical infrastructure and key assets
- Defending against catastrophic terrorism
- Emergency preparedness and response

The document elaborates in detail on planned procedures, requirements, plans and responsibilities for homeland security with regards to mentioned objectives and mission areas. Protecting critical infrastructure and key assets mission area is the crucial one from the cyber terrorisms and cyber security perspective. The strategy in this area identifies secure cyber space as one of the main initiatives. The strategy stresses the need to ensure resilient and robust security of virtual networks stated alongside the critical infrastructure. The Strategy suggests that the responsibility for security of virtual assets should be given to the Department of Homeland Security (when established). It

[220] Office of Homeland Security, *National Strategy for Homeland Security,* (Washington, White House, 2002), http://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf (accessed on 19th September 2014)

also calls for the creation of National Strategy to Secure Cyber Space, which will address this security issue in more detail.

The Strategy uses the term "cyber terrorism" only to refer to recently passed legislation in one state, but not with the reference to the actual threat it presents. Nevertheless, the document describes the possibility that terrorist will use cyber attacks as a part of their strategy: "Terrorists continue to employ conventional means of attack, while at the same time gaining expertise in less traditional means, such as cyber attacks."[221] One particular article is dedicated to the description of the possible cyber attacks launched by terrorists. It uses the argumentation that since usage of modern technologies for ideological purposes is proven, terrorist may employ this technology for more destructive purposes in the near future: "As terrorists further develop their technical capabilities and become more familiar with potential targets, cyber attacks will become an increasingly significant threat."[222] The security of information systems and other virtual assets' security are discussed in the Strategy mainly from the organizational point of view.

11.3.13. Homeland Security Act of 2002[223]

Homeland Security Act of 2002 was passed by Congress in 2002. The sole purpose of this document is to establish the Department of Homeland Security (DHS). The main responsibility of the Department is the security within American borders. Its mission currently covers following areas:

- Prevent terrorism and enhancing security
- Secure and manage American borders
- Enforce and administer our immigration laws
- Safeguard and secure cyber space
- Ensure resilience to disasters[224]

---

221 Office of Homeland Security, *National Strategy for Homeland Security,* (Washington, White House, 2002), http://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf (accessed on 19th September 2014), Executive summary

222 Ibid, Page 9

223 *H.R. 5005: Homeland Security Act of 2002,* (Washington, Congress, 2002), https://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf (accessed on 16th September 2014)

Nevertheless, some of these responsibilities were fully transferred to the Department in following years. The document itself is in deep defining the structure, organization and cooperation patterns of DHS. Cyber security within the responsibilities of DHS is described in section C – Information Security. The section is actually divided into 5 subsections:

Sec. 221. Procedures for sharing information.
Sec. 222. Privacy Officer.
Sec. 223. Enhancement of non-Federal cyber security.
Sec. 224. Net guard.
Sec. 225. Cyber Security Enhancement Act of 2002[225]

Sections 221 and 222 define procedures for information sharing and ensuring the protection of private or sensitive information. Section 223 states that DHS shall provide to State and local governments as well as to private entities related to critical information systems support, analysis and warnings related to potential threats. Section 224 establishes NET Guard, a team of subject matter expert volunteers prepared to assist with response and recovery, if needed. Section 225 actually modifies the restriction for ISPs and allows them to share personal data if they believe that there is an emergency involving danger of death or serious injury. Apart from that, this section also elaborates on cyber crime definition and prosecution, and on other related topics.

Federal Information Security Management Act of 2002 (FISMA) is also a part of the Homeland Security Act. FISMA states that it is the responsibility of every federal agency to create its cyber security strategy and implement it. Despite this freedom in addressing the cyber security issue, individual strategies and mainly implemented measures have to meet the minimal requirements set regularly by the National Institute of Standards and Technology. Office of Management and Budget was also involved not only to oversee the financial aspect, but also to supervise the security policies and practices of the agencies. DHS was involved as well as it was to be consulted when

[224] "Our Mission", Official site of the Department of Homeland Security, http://www.dhs.gov/our-mission (accessed on 28th September 2014)
[225] *H.R. 5005: Homeland Security Act of 2002,* (Washington, Congress, 2002), https://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf (accessed on 16th September 2014), Section 221 - 225

creating security standards and guidelines. The requirements are actually mandatory only for information systems identified as national security systems.[226] The Act also defines rules for the exchange of information among federal agencies and it addresses other operational issues.

The Homeland Security Act and FISMA change the approach to the terrorism threat and to other domestic security risks. On one hand it concentrates the coordination and supervision of counter-terrorist efforts (including potential cyber terrorism) in the hands of DHS, but on the other hand the FISMA leaves in general the responsibility for the implementation of security measures to individual agencies. The act de facto predestined the DHS to become a lead agency for the responsibility to secure cyber space. Nevertheless, this responsibility was confirmed later in Homeland Security Presidential Directive 7 in 2003. Establishing DHS had significant effect on the cyber security, even if not immediately, as the terrorist threat was more substantial in the physical world. It prepared necessary structures and framework as well as organizational support. FISMA created the framework and principles for the management of cyber security risks, but the effect on the actual level of cyber security was limited. Both documents do not use the term "cyber terrorism," but critical infrastructure or protected systems might become targets of computer based attacks, according to the Homeland Security Act. Therefore it acknowledges the possibility of cyber attacks.

11.3.14. Cyber Security Research and Education Act of 2002[227]

Cyber Security Research and Education Act were signed by President Bush in 2002. This bill highlights the fact that there is a shortage of qualified experts in the field o cyber security. This actually increases the vulnerability of United States to potential cyber attack. The bill therefore allocates substantial financial resources to support the education effort in this field in years 2003 – 2005 on the doctoral level.

---

[226] *H.R. 5005: Homeland Security Act of 2002,* (Washington, Congress, 2002), https://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf (accessed on 16th September 2014), Section 221 - 225, § 3542 letter (b) article 2, page 49

[227] *H.R. 3394: Cyber Security Research and Education Act of 2002,* (Washington, Congress, 2002), http://csrc.nist.gov/drivers/documents/HR3394-final.pdf (accessed on 16th September 2014)

The document uses the term "cyber terrorism" with relation to the vulnerability created by the dependence on modern technologies: "…increased reliance on technology has left our Nation vulnerable to the threat of cyber terrorism."[228] What is more important is the acknowledgement of the fact that securing cyber space requires experts in this field, but they are very scarce. This bill and the financial support it brings are trying to change this situation and motivate students to pursue PhD degree in the cyber security. Otherwise the document does not elaborate on the cyber security or possible cyber attacks.

11.3.15. National Strategy to Secure Cyber Space[229]

National Strategy to Secure Cyber Space was announced in the National Strategy for Homeland Security and it was published in 2003. It is a very extensive document addressing many aspects of the cyber security. The Strategy provides framework, which will help to protect cyber space, which is essential to American economy and American way of life. The Strategy describes three strategic objectives consistent with the Strategy for Homeland Security:

- Prevent cyber attacks against America's critical infrastructures
- Reduce national vulnerability to cyber attacks
- Minimize damage and recovery time from cyber attacks that do occur.

The Strategy confirms the Department of Homeland Security as the subject responsible for the security of cyber space on the federal level. It will also outreach to local states, nongovernmental organization, private sector, academia and public. The Department will lead the development and conduct the national threat assessment in cooperation with relevant agencies and private sector. The cooperation with private sector is highlighted in the document as the cornerstone of American cyber space security strategy. Some of the stated reasons for this partnership highlight the fact that private sector is better equipped in terms of human resources and operational flexibility to

[228] *H.R. 3394: Cyber Security Research and Education Act of 2002,* (Washington, Congress, 2002), http://csrc.nist.gov/drivers/documents/HR3394-final.pdf (accessed on 16th September 2014), section 2 article 2

[229] Department of Homeland Security, *National Srategy to Secure Cyber Space,* (Washington, 2003), https://www.us-cert.gov/sites/default/files/publications/cyber space_strategy.pdf (accessed on 2nd October 2014)

respond to rapidly evolving cyber threat. But government and appointed bodies have also their responsibility. For instance securing its own cyber infrastructure and assets supporting critical missions and services. Moreover, the government has to step in to ensure the cyber security when the transaction costs are too high or coordination is too difficult due to legal barriers.

The Strategy defines five national priorities:

- National Cyber Space Security Response System
- National Cyber Space Security Threat and Vulnerability Reduction Program
- National Cyber Space Security Awareness and Training Program
- Securing Governments' Cyber Space
- National Security and International Cyber Space Security Cooperation

The first priority focuses on the information provision and exchange consistent with privacy protection. It also states the need for tight cooperation between private and public sector in sharing information and effectively responding to possible threats. The Department of Homeland Security's United States Computer Emergency Response Team (US-CERT) was established in 2003 within the scope of this priority. The second priority describes procedures how to identify critical information systems and vulnerabilities within such systems. Moreover, the Strategy propagates best practices sharing among different sectors to address such vulnerabilities and to reduce the risk of exploitation. The third priority stresses the fact that cyber security is dependent on every actor's approach to cyber security. Individual users, companies, governmental agencies, all together create the level of national cyber security. It is therefore crucial to increase the cyber security awareness on all levels and provide training to increase the number of skilled personnel. The fourth priority describes the necessity to secure governmental networks and assets. The fifth priority addresses the special attributes of the cyber threat. The attribution problem makes it difficult to identify the attacker and adequately respond. International cooperation is necessary to increase the level of national cyber security.

The document itself does not use the term "cyber terrorism," but it states the possibility of terrorist launching cyber attacks. Therefore the sense of the term is used in the

document. The Strategy profoundly elaborates on various aspects of the cyber security and also on the threat cyber attacks present. Interestingly, this document affirms not only the importance of information systems related to critical infrastructure, but also the magnitude of cyber space itself (e.g. importance of the Internet for national economy).This Strategy indeed presents an institutional framework to ensure cyber security and in combination with other legislative documents it helps to improve the cyber security by its goals and priorities.

11.3.16. Homeland Security Presidential Directive 7[230]

Homeland Security Presidential Directive 7 was issued by President Bush in 2003. The Directive confirms the status of DHS as the leading organization for the security of cyber space and key assets. This Directive actually replaces the Presidential Decision Directive 63 (see above), which assigned coordination responsibilities to Critical Infrastructure Coordination Group and to FBI in terms of a response center. DHS is therefore recognized as the leading organization for the protection of critical infrastructure and key assets, including cyber space. The directive again highlights the necessity of cooperation with private sector to increase the level of national security.

The Directive recognizes the complexity of critical infrastructure and key assets protection, as many stakeholders are involved across different federal departments and agencies. Federal departments and agencies are therefore required to implement this Directive taking into consideration special characteristics of given sector. Furthermore, infrastructure sectors are assigned to designate Sector-Specific Agencies to oversee the implementation of security measures. The Directive also describes the process to identify critical infrastructure and key resources. It also calls for creation of National Infrastructure Protection Plan (see below).

The Directive does not mention the term "cyber terrorism," but it states the possibility of terrorist attacking critical infrastructure and key resources, including information systems and cyber space. The document therefore recognizes the possibility of terrorists launching a cyber attack. The description of the effect of possible attacks against critical

[230] George W. Bush, *Homeland Security Presidential Directive 7,* (Washington, White House, 2001), http://www.dhs.gov/homeland-security-presidential-directive-7#1 (accessed on 21st September 2014)

infrastructure and critical resources is interesting as it states apart from "conventional" effects of such attack (e.g. disruption of critical services, casualties) also "undermining the public's morale and confidence in our national economic and political institutions."[231] This effect can be assigned mainly to cyber attacks aimed against Internet and other semi-public networks, where the actual damage in terms of "conventional" effects is limited.

11.3.17. National Infrastructure Protection Plan[232]

First National Infrastructure Protection Plan (NIPP) was published in 2006 by the DHS. Following NIPPs were published by the same authority in years 2009 and 2013. NIPP was called for in the Homeland Security Presidential Directive 7 (see above).

The document presents a holistic approach to the problematic of critical infrastructure protection. Previous initiatives in this field confirmed that not only critical infrastructure might cause serious problems when attacked. Information systems, networks, Internet and other assets are referred to in NIPP as key resources (in some official publication as key assets). The NIPP therefore addresses the protection of critical infrastructure and key resources (CI/KR). Again, DHS is confirmed as the leading organization with the responsibility to develop and implement policies and measures to improve the level of security. The goal of the NIPP is defined as follows:

"Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency."[233]

To meet this goal, NIPP aims to provide a unifying structure that would incorporate existing policies and strategies and form national approach to the protection of CI/KR.

---

[231] George W. Bush, *Homeland Security Presidential Directive 7,* (Washington, White House, 2001), http://www.dhs.gov/homeland-security-presidential-directive-7#1 (accessed on 21st September 2014), page 2

[232] Department of Homeland Security, *National Infrastructure Protection Plan,* (Washington, 2006), http://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf (accessed on 2nd October 2014)

[233] Ibid, page 1, Executive Summary

NIPP presents risk management framework to address the security issues in a better way. The framework includes following activities:

- Set security goals
- Identify assets, systems, networks, and functions
- Assess risks
- Prioritize
- Implement protective programs
- Measure effectiveness

DHS will need to cooperate with various stakeholders across different industries in order to successfully execute stated activities, because of the complexity of the task. That is why the NIPP deeply elaborates on the organization of particular activities, on stakeholders' responsibilities and on coordinated approach to the security.

The cyber security issue is addressed on several places in the NIPP. Brief introduction into the problematic and description of special characteristics of cyber space are written in chapter 1.7.2 The Cyber Dimension. It also states several basic definitions used further in the document. Approach to identify critical cyber infrastructure, ergo CI/KR in cyber space, is described in chapter 3.2.5 Identifying Cyber Infrastructure. It is explained in the text that cyber infrastructure has to be approached with regard to its complexity. Cases, when the cyber infrastructure is actually spread over state boarder or across various industry sectors, present a challenge to the authorities. NIPP therefore stresses the necessity to share information both vertically and horizontally. Basic typology of information systems is also described in this part. Lack of qualified personnel in the field of cyber security is addressed in the chapter 6.3.4 Cyber Security R&D Planning. It also addresses the issue of reliable software and applications for CI/KR protection. Problem of cyber security complexity is analyzed in Appendix 1A: Cross-Sector Cyber Security.

The NIPP addresses the issue of CI/KR as such. The importance of the attacker, be it a state, group or individual is therefore reduced. Nevertheless, the document describes some of the possible threats including terrorists. But since the document is focused on the protection and it presents unifying approach to this task, the nature of the attackers

is not given that much attention. However, the type of the attacker still plays significant role on the operational level. Cyber attacks are not addressed in a big detail as the NIPP is a high level strategy. The document does not use the term "cyber terrorism," but it acknowledges the possibility that "malicious actors could conduct attacks against the cyber infrastructure using cyber attack tools."[234] NIPP focuses on the security, therefore it also elaborates on the cyber security, in the sense of another dimension where to protect critical infrastructure and as a possible primary target in terms of key resources (e.g. Internet).

11.3.18. National Security Presidential Directive 54/Homeland Security Presidential Directive 23[235]

This Directive was issued by President Bush in 2008. This Directive sets particular steps to indentify and to prepare for the future cyber attacks. It calls for a Comprehensive National Cyber Security Initiative to formulate a holistic approach to address existing vulnerabilities in the national cyber space. It also urges federal agencies to increase their effort to secure their information systems with regard to the NIPP. To promote cooperation and information sharing among FBI, CIA, USSS, NSA and other relevant agencies, the Directive orders establishing National Cyber Investigative Joint Task Force (NCIJTF) under the responsibility of FBI. NCIJTF was established in 2008. The Directive also calls for creation of National Cyber Security Center (created in 2008) within DHS to coordinate cyber security efforts within the responsibility of DHS. The Directive also includes steps to enhance the possibilities of cyber forensic analysis.

The Directive does not use the term "cyber terrorism." It mentions cyber network attacks, but it does not specify possible perpetrators. The document is focused on mobilization for better protection of cyber space against current and future threats. Organizational changes and newly created offices helped to increase the level of cyber security.

---

[234] Department of Homeland Security, *National Infrastructure Protection Plan,* (Washington, 2006), http://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf (accessed on 2nd October 2014), page 13

[235] George W. Bush, *National Security Presidential Directive 54/Homeland Security Presidential Directive 23,* (Washington, White House, 2001), https://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf (accessed on 21st September 2014)

11.3.19. Comprehensive National Cyber Security Initiative[236]

Comprehensive National Cyber Security Initiative (CNCI) was presented by President Obama in 2009. This Initiative was established by President Bush in 2008 (see above). President Obama identified cyber security as "one of the most serious economic and national security challenges we (the U.S.) face as a nation, but one that we as a government or as a country are not adequately prepared to counter."[237] President Obama ordered a 60-day review of cyber security. Regarding the results of the review, the CNCI was supported with necessary framework to ensure the implementation of CNCI actions is properly carried out. The Initiative can be regarded as a high level action plan consisting of compatible initiatives and actions with three general objectives / to establish a front line defense against immediate threats, to defend against the full spectrum of threats and to strengthen the future cyber security environment.

The actions and initiatives introduced in the CNCI are:

- Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections.
- Deploy an intrusion detection system of sensors across the Federal enterprise
- Pursue deployment of intrusion prevention systems across the Federal enterprise
- Coordinate and redirect research and development (R&D) efforts
- Connect current cyber ops centers to enhance situational awareness
- Develop and implement a government-wide cyber counterintelligence (CI) plan
- Increase the security of our classified network
- Expand cyber education
- Define and develop enduring "leap-ahead" technology, strategies, and programs
- Define and develop enduring deterrence strategies and programs
- Develop a multi-pronged approach for global supply chain risk management

---

[236] Barack Obama, *Comprehensive National Cyber Security Initiative,* (Washington, White House, 2009), http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (accessed on 21st September 2014)

[237] Ibid, Introduction

- Define the Federal role for extending cyber security into critical infrastructure domains

The CNCI introduces the necessary framework to defend against various threats and to develop more secure cyber space for the future. The document therefore does not focus on the cyber attacks; neither it uses the term "cyber terrorism." However, the initiative Define and develop enduring deterrence strategies and programs is aimed at deterring attackers – both state and non-state actors. Apart from responding to immediate cyber threats, the CNCI stresses the necessity to prepare for the future threats, also because of the rapid development of cyber space.

11.3.20. International Strategy for Cyber Space[238]

The International Strategy for Cyber Space was introduced in 2011. It is the first document describing the American approach to the cyber security within the context of international relations.

The document states that functional and reliable cyber space is vital to the American economy. Therefore US will pursue its goals in increasing the national cyber security and will internationally promote the vision of open, interoperable, secure and reliable cyber space enabling free flow of information. The importance of cyber security is increasing as the traditional offline threats moved to cyber space and present new dimension of threats to national security. Moreover, cyber threats can endanger international peace and security, as traditional forms of conflict are newly overlapping into cyber space. The Strategy therefore states that US will defend its network whether the attacks come from terrorists, criminals or states and their proxies.

US recognize the global responsibility for the cyber security, as it is not under the control of one national state. To increase the level of cyber security, US will cooperate with traditional international partners. US also offer assistance in preparation of national strategies or cyber security policies to other states sharing the American vision of open, interoperable, secure and reliable cyber space enabling free flow of information.

[238] Barack Obama, *International Strategy for Cyber Space,* (Washington, White House, 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyber space.pdf (accessed on 1st September 2014)

International cooperation is also needed to effectively tackle cyber crime. US therefore encourages other states to join the Budapest Convention on Cyber Crime. In the same time US state that general norms of responsible behavior in cyber space need to be followed. Cyber space is another dimension of the physical world and as such is within the authority of existing laws.

The document identifies cyber space as a suitable dimension for illegal activities of criminals and terrorists. The goal of American policy is to deny terrorists the ability to exploit the Internet for operational planning, financing or executing attacks against their targets.

The Strategy describes the international approach of the US towards the cyber security issue on a global level. It addresses various issues as basic human rights, cyber crime or security threats. The document does not use the term "cyber terrorism," but it acknowledges the possibility of terrorists using Internet to launch attacks. The cyber security is addressed in general mainly for the purpose to clearly demonstrate the attitude of the US to this topic. The document is very important mainly because of the fact that it clearly recognizes the collective responsibility of all states for the cyber security, as it cannot be improved without international cooperation.

11.3.21. Cyber Intelligence Sharing and Protection Act[239]

Cyber Intelligence Sharing and Protection Act (CISPA) was introduced in the Congress in 2011. It was refused by Senate in 2012 and reintroduced again in 2013, but the vote has not been taken so far. In 2014 similar bill was introduced – Cyber Security Information Sharing Act (CISA), but the vote on this bill has not been taken yet.

The aim of the CISPA and its successors is to provide Federal agencies, DHS and other governmental authorities better options to share information related to cyber security among themselves and with other stakeholders. The bill therefore mentions the necessity to share the information in the real time, the lead responsibility being given to DHS and to Federal agencies. This bill encourages the private sector to share "cyber

[239] *H.R. 3523: Cyber Intelligence Sharing and Protection Act of 2011,* (Washington, Congress, 2011), http://www.gpo.gov/fdsys/pkg/BILLS-112hr3523ih/pdf/BILLS-112hr3523ih.pdf (accessed on 16th September 2014)

threat information" with responsible authorities preferring the security to the privacy. Despite the fact that the DHS and respective agencies should report to Congress on their activities and processes to keep sensitive information, the opposition to this bill criticized this approach.

CISPA widens the perimeter for responsible agencies to gather more data and information possibly important for cyber security. It therefore does not focus on the cyber security itself, but on the coordination processes. Therefore it is not surprising that the document does not use the term "cyber terrorism." CISPA uses the term cyber threat instead and it is referring to other legal documents for the definition of this term. The document mentions cyber security mainly to describe the necessity for information sharing. The history of this document and the emotions it raised only highlight the importance cyber security gained over the years. It also highlights increasing concerns regarding individual privacy in relation to the security.

11.3.22. Presidential Policy Directive 20[240]

Presidential Policy Directive 20 was signed by President Obama in 2012. It was not published being a top secret document. Nevertheless, in 2013 it became public when The Guardian published the Directive based on information released by Edward Snowden.[241]

This Directive further elaborates on precedent legislation documents to provide coherent national policy for decisions on actions to be executed in cyber space. It also builds on the fact that Department of Defense Strategy for Operating in Cyber Space published in 2011 recognized cyber space as another dimension for military operations.[242] This Directive actually defines among others three types of operations – Defensive Cyber Effects Operations (DCEO), Nonintrusive Defensive Countermeasures (NDCM) and Offensive Cyber Effects Operations (OCEO):

---

[240] Barack Obama, *Presidential Policy Directive 20,* (Washington, White House, 2012), http://fas.org/irp/offdocs/ppd/ppd-20.pdf (accessed on 21st September 2014)

[241] Glen Greenwald, Ewen MacAskill, *Obama orders US to draw up overseas target list for cyber- attacks,* (theguardian.com, 2013), http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas (accessed on 13th October 2014)

[242] Department of Defense, *Department of Defense Strategy for Operating in Cyber Space*, (Washington, 2011), page 11, http://www.defense.gov/news/d20110714cyber.pdf (accessed on 17th September 2014)

"Defensive Cyber Effects Operations: Operations and related programs or activities - other than network defense or cyber collection - conducted by or on behalf of the United States Government, in or through cyber space, that are intended to enable or produce cyber effects outsider United States Government networks for the purpose of defending or protecting against imminent threats or ongoing attacks or malicious cyber activity against U.S. national interests from inside or outside cyber space.

Nonintrusive Defensive Countermeasures: The subset of DCEO that does not require accessing computers, information or communications systems, or networks without authorization from the owners or operators of the targeted computers, information or communications systems, or networks or exceeding authorized access and only creates the minimum cyber effects needed to mitigate the threat activity.

Offensive Cyber Effects Operations: Operations and related programs or activities - other than network defense, cyber collection, or DCEO - conducted by or on behalf of the United States Government, in or through cyber space that are intended to enable or produce cyber effects outsider United States Government networks."[243]

The Directive states that DCEO and OCEO must be executed only in consistence with the obligations given by international law and the law of armed conflict, with regard to national sovereignty and neutrality. The document also defines the decision process and responsibilities for such actions. Ordinary actions such as cyber collection (gathering of intelligence) or NDCM are already addressed in existing processes of management by relevant agencies. OCEO or DCEO may be used in military actions approved by the President according, but OCEO or DCEO actions that will possibly produce cyber effects within US require President's approval. President's approval is also needed for actions with possible significant consequences (loss of life, significant damage to property, serious adverse US foreign policy consequences, or serious economic impact on US[244]). The exception is an emergency situation. Emergency cyber actions can be executed

[243] Barack Obama, *Presidential Policy Directive 20,* (Washington, White House, 2012), page 3, http://fas.org/irp/offdocs/ppd/ppd-20.pdf (accessed on 21st September 2014)
[244] Ibid, page 10

within the authority of responsible department or agency director. These actions may involve also OCEO or DCEO otherwise requiring the President's approval.

One of the stated reasons for the policy described in this Directive is the global aspect of cyber space. Cyber operations, especially DCEO and OCEO, might have unintended or collateral consequences, given the nature of cyber space. Therefore the conduct of such operation must be consistent with legal obligations as stated above, but also with the values and principles described in the International Strategy for Cyber Space (see above). Therefore US Government shall obtain consent from countries possibly affected by cyber operations, unless US is acting in self defense or the exception is approved by President or such operations are executed within the mandate of military operations already approved by the President.

Despite the fact that OCEO can be more efficient or more suitable than other type of operations, the document acknowledges the fact that development and sustainment of OCEO capabilities will require considerable time and effort.

The Directive also instructs responsible departments and authorities to produce criteria and procedures how to respond to malicious cyber activities against US interests. These shall be approved the President. This framework will enable responsible departments and authorities to efficiently react to possible threats.

This Directive is very important as it clearly confirms that fact that US will use cyber offensive measures if needed or necessary and not only for immediate protection; such actions might be used in military campaigns. It establishes framework for decision making for actions with possible collateral consequences. It also provides guidelines to responsible departments and authorities and it calls for creation of criteria and procedures. These are necessary to define to which extent the departments and authorities can act without the need of further approval. As this Directive focuses on the processes, it does not stress the threat of possible terrorists' cyber attacks. The term "cyber terrorism" is not mentioned in the document. The nature of the threat is not discussed neither.

11.3.23. Executive Order 13636[245]

Executive Order 13636 was issued by President Obama in 2013. The main purpose of this order is to further improve the protection of critical infrastructure from cyber attacks through increased sharing of information. It calls for creation of cyber security incidents reports by DHS and National Intelligence to be accessible also by private companies and other stakeholders. These reports are to be produced regularly. It also calls for a report from DHS on the risks of violation of privacy and civil liberties by DHS's activities and programs.

The Order also establishes the Voluntary Critical Infrastructure Cyber Security Program. This program will motivate operators of critical infrastructure and other private companies to accept advice and counseling regarding cyber security from sector specific agencies. It also calls for new, more efficient framework for critical infrastructure cyber security and information sharing. The Order also calls for a review of current legislation.

This Order focuses on the critical infrastructure protection from the cyber threats. It elaborates on the information sharing and on the increased effort to motivate private sector to improve their cyber security. It also demonstrates the tendency of focus on the cyber security itself disregarding the threat. The reason might be that the systems' protection principles are the same disregarding the nature of the threat or attack. The Order therefore does not use the term "cyber terrorism." It does not mention cyber attacks neither. It highlights increased cyber threats as a reason for increased effort in securing critical infrastructure.

11.4. Summary

Analyzed documents recognize the possibility of cyber attacks (computer based attacks) in 1996 in the Executive Order 13010 issued by President Clinton. Despite the fact that this document focuses on the protection of critical infrastructure, it acknowledges the fact that critical infrastructure heavily uses information systems and information networks, which might be potential targets. Analyzed documents from years prior to 1996 concern firstly computer and data security. This is particularly visible from

[245] Barack Obama, *Executive order 13636,* (Washington, White House, 2012), http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (accessed on 21st September 2014)

documents Federal Computer Systems Protection Act (1977) and Computer Security Act (1989). The main threat is infection of viruses, lack of control over automated processed and data protection. Between 1989 and 1996, the network principle became to be more important. Of course that data and computer protection were still important, but the fact that the systems were becoming more and more interconnected started to be a security issue, particularly with regards to critical infrastructure. The possibility that terrorists might use cyber attacks first appeared in 1998 in the Presidential Decision Directive 62. Cyber warfare was recognized as one of the unconventional threat in this document, possibly used by terrorist. Since then majority of documents on the topic of cyber security or critical infrastructure protection acknowledges terrorists as a possible source of cyber attacks. But the term "cyber terrorism" had to wait till the threat of terrorism gained larger attention. This happened with the 9/11 attacks. The USA Patriot Act followed shortly after the attacks in 2001 and used the term for the first time in the analyzed documents. It is no wonder that the term is used in this document establishing the basics of American counter-terrorism policy. Terrorists and their actions were analyzed in detail and cyber terrorism was one of their options.

Cyber security is currently regarded as a very important topic, especially in relation to the increasing magnitude of cyber space. Some 30 years ago, the situation was different. Computers were used on a larger level and also in critical infrastructure. Malfunctions or errors of these computers caused by viruses, wrong orders or human mistakes were considered as a serious threat in the 80s. With the networking aspect and the increased usage in the critical infrastructure, cyber security became an important feature of critical infrastructure protection. It is described as such in President Clinton's Decision Directives number 62 and 63. During that time the Internet was on rise. Number of users was dramatically increasing all over the world and the Internet bubble (.com bubble) was about to reach its climax in 2000. Cyber space, mainly its component the Internet, was becoming more and more important to national economies and to the way of life. This was true especially in the U.S., where the Internet boom begun. It not surprising, that in parallel to this increase of cyber space importance, cyber security became an independent topic. It was mentioned as such for the first time in the analyzed documents in 2000 in the National Plan for Information and Systems Protection. The document clearly stated the dependency of the U.S. on cyber space and therefore also its intention

to secure it. During the last decade cyber security became an independent topic within the American security policy.

Based on the information stated above, it is possible to say that the hypothesis for this chapter has been rejected. Cyber terrorism is addressed in the documents influencing American security policy since 1998, when terrorists were identified as a possible source of cyber attacks. Cyber security is even recognized as an independent and unique topic of national security.

12. Conclusion

The dissertation has actually confirmed that the definition of terrorism is applicable also to cyber attacks, and therefore cyber terrorism is a subtype of terrorism. Statistical analysis of the number of terrorist attacks and terrorist groups has brought very interesting information. On the general level, the analysis has showed that the threat of terrorism still exists despite the ongoing war on terror. Moreover, the number of terrorist attacks has increased on the global level. But the analysis has not confirmed the hypothesis that existing terrorist groups are forced to seek new types of attack because of a decline in the success rate. Every terrorist attack has to be analyzed independently to determine the probability of success. These research results discredits one of the reasons for which terrorists develop new techniques of attack (decreasing probability of attacks' success), but other reasons remain. The most important is the motivation to cause maximal damage by a surprising attack. Low number of terrorist attacks committed in the U.S. and the high dependency on cyber space might motivate terrorists to develop cyber attack capabilities or to procure them. The case study analysis has revealed that cyber attacks can be even more dangerous than "conventional" terrorist attacks despite particular characteristics of such attacks. The comparison has showed that the position of the U.S. in cyber space is significantly different from its position in the physical world. High dependency on modern technologies and on cyber space makes the U.S. vulnerable in cyber space, until adequate security measures are adopted. The study of important documents shaping the American security policy confirmed that cyber terrorism is recognized in some of these documents. Moreover, the analysis has found important facts about the evolution of the approach to the threat of cyber attacks.

The risk of cyber terrorism is not limited only to existing terrorist organization. New groups of hackers that can be under certain conditions regarded as terrorists have emerged and increased the security risk in relation to cyber space. These attackers are not regarded as a terrorist group because they have not committed any terrorist attack yet. They are not on the lists published by American or European authorities. However, their actions might be monitored mainly for their cyber crime potential. It is important to realize that these "new" terrorists would not commit a physical attack, but they are willing to engage in possibly dangerous cyber activities. They do not need to be centrally organized. Individual hackers might join particular attacks or activities as they please.

Attackers might be also supported by a state or even belong to specialized units trained explicitly to commit cyber attacks. Many states have officially declared that they are pursuing activities to create or improve their military capabilities in cyber space. Other states benefit from the special skills of their citizens and create voluntary teams of experts that are ready to assist state authorities in case of major cyber attacks. Another approach is to engage national hackers to cooperate with official authorities and assist them in some operations.

In such cases, the distinction of cyber terrorism as a separate threat to national security starts to lose its importance. This is even further supported by the findings that existing terrorist groups would tend to a particular type of attacks relying on pure strength, whereas state supported groups would actually commit more complex and more dangerous cyber attacks.

When considering all mentioned findings of the dissertation, it is necessary to question the importance of cyber terrorism as an independent threat to the U.S. security. It is possible to use the analogy from the threat of terrorism. Terrorism is defined from several reasons.

Firstly, its legal interpretation enables security forces to efficiently investigate terrorists and perform counter-terrorism activities. Different approach is taken when the criteria of the definition of terrorism are met. Secondly, terrorism is defined as a security threat because it differs from existing threats and particular security measures must be implemented.[246] This relates mainly to the fact that terrorists' goal is to spread terror. Existing practice is to attack civilian targets to inflict significant damage or to cause casualties, thus disrupting normal way of life. The selection of targets differentiates

[246] Particular security measures can be illustrated on the example of walls in Israel. Such measure is useless against regular army or against petty criminals. But under local particular circumstances it reduced the number of terrorist attacks, at least for a while. Another example might be the installation of CCTV systems in public places in the U.S. Of course that it helps Police to fight common criminals, but different patterns of behavior are observed to identify potential terrorists. The last example of particular approach needed to fight terrorism is the phenomena of suicide attackers, when the standard security checkpoints are perfect targets from the terrorists' perspective.

terrorist attacks from military actions or from criminal acts. Thirdly, terrorists use very violent methods of attack often disregarding their own security.

The definition of cyber terrorism from the legal perspective does not bring any advantages to the security forces. Since cyber terrorism is a type of terrorism, the definition of terrorism is sufficient to perform the same actions as when investigating "common" terrorism.

The difference is the motivation of the attackers. Nevertheless, this difference does not influence the security measures or processes. It is not important whether the motivation of the attacker is compliant with the definition of terrorism as long as targets and methods are the same for terrorists and other perpetrators.

Cyber terrorism uses the same tools and methods that are used by other attackers, be it hackers, criminals or states. There is no special kind of cyber attacks comparable to a suicide bomber in the physical world. Attackers use basic tools adapted for a particular attack. It is very often a combination of different means and methods deployed to breach a particular system and reach the attacker's goal. Moreover, the research showed that the most complex attacks are more likely to be launched by groups with state support or by states themselves.

Targets are chosen according to attacker's goal and motivation. It has been said that the motivation does not influence the selection of methods. The goal is the same in cyber space as well as in the physical world – spread fear and terror, disrupt the normal way of life. The selection of targets for cyber attacks is very wide, but the limiting factor is the connection to the cyber space or usage of modern ICTs. In other words, cyber attacks can be used only against targets connected to the cyber space or targets operated by computer systems. Taking into consideration committed terrorist attacks in the physical world, the way how to spread fear and terror is to inflict civilian casualties or to disrupt the normal way of life. Both alternatives are in cyber space related to critical infrastructure. This leads to SCADA systems and other critical infrastructure systems and networks. Some of security incidents related to these possible targets have been analyzed in the form of case studies. It is visible from the results that these systems have

to be well protected not only because of possible terrorists' cyber attacks, but also from malfunction, uncontrolled viruses and possibly attacks executed by other perpetrators than terrorists. Practically all potential targets for terrorists have been already identified as potential targets of cyber criminals, hackers or other types of attackers. In this case, the differentiation of cyber terrorism does not bring any new possible targets that have to be protected from cyber attacks launched exclusively by terrorists. Of course that terrorists will seek to find new targets that are not yet on the list. But so will hackers and other attackers. Not even mentioning uncontrolled viruses that target practically all systems in range.

Differentiation of cyber terrorism as a threat to the U.S. security does not bring any new legal advantages for investigation and implementation of counter measures, as cyber terrorism is a type of terrorism. Terrorism has remained among main threats to the U.S. security and therefore it is not necessary to distinguish cyber terrorism from the legal perspective. Neither it brings any new possible targets that would need to be specially secured against cyber terrorists or any new tools or methods of attacks. General threat of cyber attacks covers also the security aspects of cyber terrorism. In other words cyber terrorism is indeed a threat, but only as a possible source of cyber attacks.

It is very important that cyber security is actually recognized as a threat to the U.S. Cyber security together with the threat of terrorism covers all the security aspects related to cyber terrorism. In case the one of the threat would not be included in the U.S. security policy and subsequently all legal and security measures would be removed, cyber terrorism would become a very dangerous threat and it would be necessary to recognize cyber terrorism as a threat to the U.S. security in relevant documents. The reason would be that security measures based on such policy missing the threat of terrorism or cyber attacks would not count either with cyber attacks or would not grant increased powers to investigate cyber terrorists.

Supporting evidence in favor of this conclusion was found during the analysis of the key documents shaping the American security policy. Cyber terrorist have been always mentioned as a possible source of cyber attacks. Moreover, in the most recent documents cyber security is recognized as an independent threat of major importance.

Despite the fact that the importance of cyber terrorism as an independent threat to the U.S. security have been just questioned, research findings actually suggest that a new type of terrorists has appeared. These terrorists are group of hackers. Their actions under particular conditions can be regarded as terrorist activities. It is true that they can be simply labeled as terrorist in the general meaning of the term. Nevertheless, future research might confirm that it is convenient to create a new term for these individuals or groups. Since they are not active outside cyber space, placing them on the same level as existing terrorist groups would be incorrect simplification. Term cyber terrorists actually depict these potential attackers. Whereas existing terrorist might include cyber attacks into their methods, for cyber terrorists are cyber attacks the only possible means. This differentiation would be useful to determine the action radius of both different groups.

The dissertation defined cyber terrorism and found that it indeed presents a threat to the U.S. security, but only as one possible source of cyber attacks. Since both issues – terrorism and cyber security are reflected in the U.S. security policy, the identification f cyber terrorism as an individual threat to the U.S. security is redundant. The approach of the U.S. towards the threat of cyber terrorism is in the form of consolidated approach ensuring robust cyber security on a general level, which will defend the U.S. cyber space not only against terrorists, but against all possible perpetrators using cyber attacks.

The dissertation has not answered all asked question positively. Despite the fact that terrorism is still a threat to the U.S. security, no factual evidence was found to confirm the hypothesis that existing terrorists will start using cyber attacks because of the decrease in the success rate of their current attacks. Moreover, the analyses of the case studies has revealed that cyber attacks might be regarded as threat in general, thus discrediting the importance of cyber terrorism as a standalone threat to the U.S. security. The focus therefore has to be on general cyber security rather than on security measures implemented to defend against particular source of cyber attacks.

The research question was answered only partially. Evidence was found to recognize cyber terrorism as a threat to the U.S. security, but cyber terrorism is approached more

as a source of cyber attacks. The importance of cyber terrorism as a clearly defined threat has been rejected. Cyber attacks are in general addressed by cyber security measures and related activities. The identification of cyber terrorism as a possible threat therefore loses its importance, because it does not influence the security per se.

Despite this conclusion, the dissertation presented very important findings for further research and discussion. Apart from the definition of terrorism and cyber terrorism, statistical findings should inspire further research exploring statistical models in terrorist actions to better understand the existing trends. Attention should be given to newly emerged groups of hackers who could possible cross the line and become terrorist groups posing a severe risk to the U.S. security. The analysis of case studies demonstrated the importance of cyber security due diligence and it should serve as trigger to explore the role of the state in setting security standards and managing the national cyber security. The overview of crucial documents shaping the U.S. security policy should serve as an introduction for comparative studies focusing on different national strategies addressing cyber security.

13. List of tables, pictures and charts

14. Bibliography

14.1. Publications

ABRAHMS, Max, The Political Effectiveness of Terrorism Revisited, (Comparative Political Studies, 2012), [http://cps.sagepub.com/content/45/3/366,] (accessed 21st November 2013);
ABRAMS, Marshall, WEISS, Joe, *Bellingham, Washington DC, Control System Cyber Security Case Study*, (Mitre/NIST, 2007), [http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Bellingham_Case_Study_report%2020Sep071.pdf] (accessed on 27th November 2013);
ABRAMS, Marshall, WEISS, Joe, *Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia,* (Mitre/NIST, 2008), [http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf] (accessed on 17th September 2013);
ANONYMOUS, *Maximum Security: A Hacker's Guide to Protecting Your Computer Systems and Network*, (Sams: Indianapolis, 2002);
BAIER, Bret, PORTEUS, Liza, *Thousands of Iraqui Troops Appear Ready to Surrender,* (Fox News, 2003), [http://www.foxnews.com/story/2003/03/19/thousands-iraqi-troops-appear-ready-to-surrender/] (accessed on 21st March 2013);
BELL, Steve, *Which is the worst computer virus in history? Here's our top 10,* (BullGuard: United Kingdom, 2014), [http://www.bullguard.com/blog/2014/03/which-is-the-worst-computer-virus-in-history-heres-our-top-10.html] (accessed 6th June 2014);
BERGEN, Peter L., *September 11 attacks,* (Britannica.com, 2014), [http://www.britannica.com/EBchecked/topic/762320/September-11-attacks] (accessed on 18th February 2014);
BIRD, Jim, *Bugs and numbers: How many bugs do you have in your code?,* (Building Real Software, 2011), [http://swreflections.blogspot.cz/2011/08/bugs-and-numbers-how-many-bugs-do-you.html] (accessed 13th June 2014);
BOWMAN, Steve, *Weapons of Mass Destruction: The Terrorist Threat,* (Congressional Research Service, 2002), [http://fpc.state.gov/documents/organization/9184.pdf] (accessed 24th September 2014)
BRADLEY, Mitchell, *Protocol (Network),* (About technology, 2010), [http://compnetworking.about.com/od/networkprotocols/g/protocols.htm] (accessed on 17th September 2013);
BRANIGAN, Tania, *Chinese astronauts complete successful docking at space lab,* (The Guardian: London, 2012), [http://www.guardian.co.uk/world/2012/jun/18/chinese-astronauts-complete-space-docking] (accessed on 8th September 2012);
BUNTER, Bill, *How to Protect Against Social Engineering Attacks,* (Bright Hub, 2012), [http://www.brighthub.com/computing/smb-security/articles/1313.aspx] (accessed on 19th September 2013)
BUSH, George W., *Executive Order 13228,* (Washington DC, The White House, 2001), [http://georgewbush-whitehouse.archives.gov/news/releases/2003/01/text/20030124.html] (accessed on 21st September 2014);
BUSH, George W., *Homeland Security Presidential Directive 7,* (Washington DC, The White House, 2001), [http://www.dhs.gov/homeland-security-presidential-directive-7#1] (accessed on 21st September 2014);
BUSH, George W., *National Security Presidential Directive 54/Homeland Security Presidential Directive 23,* (Washington DC, The White House, 2001), [https://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf] (accessed on 21st September 2014);
CAPACCIO, Tony, TIRON, Roxana, *North Korea's cyber warfare capability grows, U.S. general says,* (Bloomberg News, 2012), [http://www.staradvertiser.com/news/breaking/144695475.html?id=144695475] (accessed on 11th August 2012);
CAVELTY, Myriam Dunn, *Cyber-Security and Threat Politics*, (Routledge: New York, 2008);
CLARK, David, *Characterizing Cyberspace: Past, Present and Future,* (MIT/CAIL 2010), [https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyber space_1-2r.pdf] (accessed on 18th July 2013);
CLARKE, Richard A., KNAKE, Robert K., *Cyber War*, (HarperCollins: New York, 2010);

CLINTON, Hillary, *Remarks on Internet Freedom,* (U.S. Department of State, 2010), [http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm] (accessed on 24th November 2011);
CLINTON, William J., *Executive Order 13010 – Critical Infrastructure Protection,* (Washington DC, The White House, 1996), [http://fas.org/irp/offdocs/eo13010.htm] (accessed 14th September 2014);
CLINTON, William J., *Presidential Decision Directive 62,* (Washington DC, The White House, 1998), [http://fas.org/irp/offdocs/pdd/pdd-62.pdf] (accessed 14th September 2014);
CLINTON, William J., *Presidential Decision Directive 63,* (Washington DC, The White House, 1998), [http://fas.org/irp/offdocs/pdd/pdd-63.html] (accessed 14th September 2014);
CLULEY, Graham, *Feedly refuses to give in to blackmail demands, gets hit by DDoS attack,* (Cluley Associates Limited: United Kingdom, 2014), [http://grahamcluley.com/2014/06/feedly-blackmail-ddos/] (accessed 5th August 2014);
CLULEY, Graham, *Internet firm goes out of business after DDoS exortion attack,* (Eset, 2014), [http://www.welivesecurity.com/2014/06/21/internet-firm-ddos-extortion-attack/] (accessed 21st August);
CLUTTERBUCK, Lindsay, *Terrorists Have to Be Lucky Once; Targets, Every Time,* (rand.org, 2008), [http://www.rand.org/blog/2008/11/terrorists-have-to-be-lucky-once-targets-every-time.html] (accessed on 9th October 2012);
COLARIK, Andrew, *Cyber Terrorism: Political and Economic Implications,* (Idea Group Publishing: London, 2006);
CROOK, Jordan, *Infamous Hacker Creates SkyJack To Hunt, Hack, And Control Other Drones,* (techcrunch.com, 2013), [http://techcrunch.com/2013/12/04/infamous-hacker-creates-skyjack-to-hunt-hack-and-control-other-drones/] (accessed on 18th May 2014);
DE LA CORTE IBANEZ, Luis, *Logika Terorismu*, (Academia : Praha, 2009);
DOUGHTY-WHITE, Pearl, QUICK, Miriam, *Codebases*, (Informationisbeautiful, 2013), [http://www.informationisbeautiful.net/visualizations/million-lines-of-code/] (accessed 18th July 2014);
DUGGAN, Maeve, SMITH, Aaron, *Social Media Update 2013,* (The Pew Research Center: Washington DC, 2014),[http://www.pewinternet.org/files/2013/12/PIP_Social-Networking-2013.pdf] (accessed on 29th June 2014);
ESCOBEDO, Tricia, *Nun, two others in federal court for nuclear breach,* (CNN.com, 2013), [http://edition.cnn.com/2013/05/07/justice/nun-nuclear-breach-charges/] (accessed on 21st September 2013);
ESPINER, Tom, *Georgia accuses Russia of coordinated cyberattack,* (cnet, 2008), [http://www.cnet.com/news/georgia-accuses-russia-of-coordinated-cyberattack/] (accessed on 20th March 2013);
FISHER, Max, *Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?,* (washingtonpost.com, 2013), [http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/] (accessed on 28th September 2013);
FOREST, James, *Framework for Analyzing the Future Threat of WMD Terrorism,* (Journal of Strategic Security, 2012), [http://scholarcommons.usf.edu/jss/vol5/iss4/9/, page 51-68] (accessed 24th September 2014);
GALLARGHER, Sean, *Chinese hackers steal Indian Navy secrets with thumbdrive virus,* (arstechnica, 2012), [http://arstechnica.com/security/2012/07/chinese-hackers-steal-indian-navy-secrets-with-thumbdrive-virus/] (accessed 9th August 2012);
GEERS, Kenneth, et al., *World War C : Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks,* (FireEye, 2014), [http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf] (accessed on 15th September 2014);
GJELTEN, Tom, *Could Iran Wage A Cyberwar On The U.S.?,* (National Public Radio, 2012), [http://www.npr.org/2012/04/26/151400805/could-iran-wage-a-cyberwar-on-the-u-s] (accessed on 10th August 2012);
GORMAN, Siobhan, *Fraud Ring Funnels Data From Cards to Pakistan*, (wallstreetjournal.com, 2008), [http://online.wsj.com/news/articles/SB122366999999723871] (accessed on 21st September 2013);
GOSTEV, Alexander, *The Flame: Questions and Answers,* (Kaspersky lab: Russian Federation, 2012), [http://securelist.com/blog/incidents/34344/the-flame- questions-and-answers-51/] (accessed on 29th June 2013);
GREENWALD, Glenn, *How would a Patriot Act*, (Working Assets Publishing: USA, 2006);

GREENWALD, Glen, MACASKILL, Ewen, *Obama orders US to draw up overseas target list for cyber- attacks,* (theguardian.com, 2013), [http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas] (accessed on 13th October 2014);
GREENHOUSE, Linda, *O'Connor Foresees Limits on Freedom,* (New York Times, 2001), [http://www.nytimes.com/2001/09/29/national/29SCOT.html] (accessed on 21st February 2013);
HENRY, David, FINKLE, Jim, *JPMorgan warns 465.000 card users on data loss after cyber attack,* (reuters.com, 2013), [http://www.reuters.com/article/2013/12/05/us-jpmorgan-dataexposed-idUSBRE9B405R20131205] (accessed on 5th January 2014);
HERN, Alex, *North Korean 'cyberwarfare' said to have cost South Korea £500m,* (theguardian.com, 2013), [http://www.theguardian.com/world/2013/oct/16/north-korean-cyber-warfare-south-korea] (accessed on 20th October 2013);
HISKMAN, Martin, *Online protest drive Nestlé to environmentally friendly palm oil,* (Independent: United Kingdom, 2010), [http://www.independent.co.uk/environment/green-living/online-protest-drives-nestl-to-environmentally-friendly-palm-oil-1976443.html] (accessed 15th June 2014);
HUNGTINGTON, Samuel P., *The Clash of civilizations?*, (Simon&Schuster: New York, 1996);
JANCAR, Rosťa, *Americké letectvo testuje pilotní mapy na vojenských iPadech mini,* (idnes.cz, 2013), [http://technet.idnes.cz/letectvo-mapy-ipad-0n5-/notebooky.aspx?c=A130731_192627_tec_technika_rja] (accessed on 21st September 2013);
KATZ, Raul, *The Impact of Broadband on the Economy: Research to Date and Policy Issues,* (ITU: Columbia, 2012), [http://www.itu.int/ITU-D/treg/broadband/ITU-BB-Reports_Impact-of-Broadband-on-the-Economy.pdf] (accessed on 25th April 2014);
KERR, Paul K., *Nuclear, Biological, and Chemical Weapons and Missiles: Status and Trends,* (Congressoinal Research Service, 2008), [http://fas.org/sgp/crs/nuke/RL30699.pdf] (accessed 5th May 2012);
KESLER, Brent, *The Vulnerability of Nuclear Facilities to Cyber Attack; Strategic Insights: Spring 2010,* (Naval Postgraduate School: Monterey, 2011), [http://hdl.handle.net/10945/25465] (accessed on 15th July 2013)
KOHUT, Andrew, et al., *In Changing News Landscape, Even Television is Vulnerable,* (The Pew Research Center: Washington DC, 2012), [http://www.people-press.org/files/legacy-pdf/2012%20News%20Consumption%20Report.pdf] (accessed on 6th February 2013);
KRAMER, Franklin D., et al., eds., *Cyberpower and National Security*, (Potomac Books: Dulles, 2009);
KURBALIJA, Jovan, *An Introduction to Internet Governance*, (DiploFoundation: Geneva, 2014) ;
LAZNOVSKY, Matouš, *Chybu zveřejněnou expertem Googlu využili hackeři před vydáním opravy,* (Mafra: Prague, 2013), [http://technet.idnes.cz/microsoft-oprava-chyby-0v1-/sw_internet.aspx?c=A130710_165204_sw_internet_mla] (accessed 26th June 2014);
LEE, Laurie Thomas. *The USA PATRIOT Act and telecommunications: privacy under attack*. (Rutgers Computer & Technology Law Journal 29.2, 2003);
LIA, Brynjar, *Globalization and the Future of Terrorism*, (Routledge: USA, 2005);
LOCKE, John, *Second Treatise of Civil Government*, (Cambridge University Press: Cambridge, 1960);
LYMAN, Peter, VARIAN, Hal R., *How Much Information,* (University of California at Berkley: California, 2003), [http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/printable_report.pdf/] (accessed on 29th June 2013);
MACASKILL, Ewen, *Julian Assange like a hi-tech terrorist, says Joe Biden,* (guardian.com: Washington DC, 2010), [http://www.theguardian.com/media/2010/dec/19/assange-high-tech-terrorist-biden] (accessed on 13th February 2012);
MANGOLD, Tom, GOLDBER, Jeff, *A mnoho lidí zemřelo...pravda o biologických válkách*, (Themis: Praha, 2001);
MARGULIES, Joseph, *Guantanamo and the abuse of Presidential Power*, (Simon & Schuster: USA, 2006);
MARKS, Paul, *Air traffic system vulnerable to cyber attack,* (newscientist.com, 2011), [http://www.newscientist.com/article/mg21128295.600-air-traffic-system-vulnerable-to-cyber-attack.html#.VGyzxskt1Gd] (accessed on 17th September);
MCBORROUGH, William, *The Need for Improved Critical Infrastructure Protection,* (infosec island, 2012), [http://www.infosecisland.com/blogview/21616-The-Need-for-Improved-Critical-Infrastructure-Protection.html] (accessed on 15th September 2012);
MONROE, John , Forecast Analysis: Hard-Disk Drives, Worldwide, (The Gartner, 2013), [http://www.gartner.com%2Fdoc%2F2583019%2Fforecast-analysis-harddisk-drives-worldwide&ei=_gFxVMCsNoj1OM3CgNAD&usg=AFQjCNF0RhW9ZrhAfP-6S9xu4iohi_2OwA&bvm=bv.80185997,d.ZWU] (accessed on 9th September 2013);
MOSKVITH, Katia, *Are drones the next target for hackers?,* (bbc.com, 2014), [http://www.bbc.com/future/story/20140206-can-drones-be-hacked] (accessed on 5th June 2014);

MOTEFF, John D., *Critical Infrastructures: Background, Policy, and Implementation,* (Congressional Research Service, 2014), [http://fas.org/sgp/crs/homesec/RL30153.pdf] (accessed on 21st September 2014);
MUELLER, John, and STEWART, Mark G., *Balancing the Risks, Benefits, and Costs of Homeland Security,* (Homeland Security Affairs, 2011), [https://www.hsaj.org/articles/43] (accessed on 19th February 2013);
MURDICO, Vinnie, *Bugs per line of code,* (Tester's World, 2007), [http://amartester.blogspot.cz/2007/04/bugs-per-lines-of-code.html] (accessed 23rd June 2014);
NYVLT, Vaclav, *Důchodkyně šla "na dřevo", pilkou odřízla dva státy od internet,* (technet.cz, 2011), [http://technet.idnes.cz/duchodkyne-sla-na-drevo-pilkou-odrizla-dva-staty-od-internetu-p61-/sw_internet.aspx?c=A110411_092852_sw_internet_nyv] (accessed on 16th July 2013);
OBAMA, Barack, *Comprehensive National Cyber Security Initiative,* (Washington DC, The White House, 2009), [http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative] (accessed on 21st September 2014);
OBAMA, Barack, *Executive order 13636,* (Washington DC, The White House, 2012), [http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf] (accessed on 21st September 2014);
OBAMA, Barack, *International Strategy for Cyber Space,* (Washington DC, The White House, 2011), [http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyber space.pdf] (accessed on 1st September 2014);
OBAMA, Barack, *Presidential Policy Directive 20,* (Washington DC, The White House, 2012), [http://fas.org/irp/offdocs/ppd/ppd-20.pdf] (accessed on 21st September 2014);
OCHRANA, František, *Metodologie vědy*, (Karolinum: Prague, 2009);
ORR, Bob, *U.S. official: Iran does have our drone,* (cbsnews.com, 2011), [http://www.cbsnews.com/news/us-official-iran-does-have-our-drone/] (accessed on 5th February 2012);
PAUL, Don J. H., *The World Trade Center Attack,* (911review, 2011), [http://www.911review.com/attack/wtc/index.html] (accessed on 5th May 2011);
PEREZ, Sarah, *Facebook Looking Into Buying Drone Maker Titan Aerospace,* (techcrunch.com, 2014), [http://techcrunch.com/2014/03/03/facebook-in-talks-to-acquire-drone-maker-titan-aerospace/] (accessed on 5th June 2014);
PERRIN, Chad, *The danger of complexity: More code, more bugs,* (CBS Interactive: United States, 2010), [http://www.techrepublic.com/blog/it-security/the-danger-of-complexity-more-code-more-bugs/] (accessed 17th June 2014);
PETERSON, Andrea, POOL, Sean, *Timeline: U.S. Cyber Security Policy in Context,* (Science Progress, 2013), [http://scienceprogress.org/2013/02/u-s-cybersecurity-policy-in-context/] (accessed on 2nd September 2014);
PETERSON, Scott, FARAMAZI, Payam, *Exclusive: Iran hijacked US drone, says Iranian engineer,* (csmonitor.com, 2011), [http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video] (accessed on 5th January 2012);
PLETCHER, Kenneth, *Tokyo subway attack of 1995,* (Britannica.com, 2014), [http://www.britannica.com/EBchecked/topic/1669544/Tokyo-subway-attack-of-1995] (accessed on 5th March 2014);
PONT, Simon, *Digital State*, (KoganPage: London, 2013);
POTTER, Will, *FBI Arrests 4 Activists as "Terrorists"for Chalking Slogans, Leafleting and Protesting,* (Green is the New Red, 2009), [http://www.greenisthenewred.com/blog/aeta-arrests/1070/] (accessed 21st July 2014);
PRENTICE, Stephen, *The Future of the Internet: The Three Forces Shaping the Internet and How They Will Affect Your Business,* (The Gartner, 2012), [http://www.gartner.com%2Fdoc%2F2118015%2Ffuture-internet-forces-shaping-internet&ei=3QJxVNe2F4ffPfS1gOgB&usg=AFQjCNG-Tunf76RI46LkrJRKXf2eby1_Ew&bvm=bv.80185997,d.ZWU] (accessed on 17th October 2013);
RANGER, Steve, *Hostile state-sponsored hackers breached government network,* (ZDnet.com, 2014), [http://www.zdnet.com/hostile-state-sponsored-hackers-breached-government-network-7000030619/] (accessed on 14th September 2014);
RAY, Michael, *London bombings of 2005,* (Britannica.com, 2013), [http://www.britannica.com/EBchecked/topic/1696348/London-bombings-of-2005] (accessed on 15th October 2013);
REED, Brad, *Internet cable cuts raise alarms over infrastructure vulnerabilities,* (NetworkWorld, 2008), [http://www.networkworld.com/article/2282941/lan-wan/internet-cable-cuts-raise-alarms-over-infrastructure-vulnerabilities.html] (accessed on 19th November 2013);

REZEK, Tomas, *Přinese nový prezident Spojeným státům bezpečnější kyberprostor?,* (NATOAktual.cz, 2012), [http://www.natoaktual.cz/prinese-novy-prezident-spojenym-statum-bezpecnejsi-kyberprostor-1dr-/na_analyzy.aspx?c=A120904_074755_na_analyzy_m02] (accessed on 4th September 2012);
RIBEIRO, John, *US charges 13 Anonymous members for DDoS attack,* (PCWorld: United States, 2013), [http://www.pcworld.com/article/2052360/us-indicts-13-anonymous-members-for-ddos-attacks.html] (accessed 8th July 2014);
RICHARDS, Jason, *Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security,* (Elliot School of International Affairs, 2007), [http://www.iar-gwu.org/node/65,] (accessed on 5th October 2013);
RID, Thomas, *Cyber War Will Not Take Place,* (Hurst&Company: London, 2013);
RILEY, Michael, LAWRENC, Dune, *Hackers Linked to China's Army Seen From EU to D.C.,* (Bloomberg News, 2012), [http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html] (accessed on 9th August 2012);
ROLLINS, John, *Terrorist Use of the Internet: Information Operations in Cyberspace,* (Congressional Research Service, 2011), [http://fas.org/sgp/crs/terror/R41674.pdf,] (accessed on 20th April 2013);
SHACHTMAN, Noah, *Exclusive: Computer Virus Hits U.S. Drone Fleet,* (wired.com, 2011), [http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/] (accessed on 17th September 2013);
SANDLER, Todd, *The Past and Future of Terrorism Research*, (CREATE, 2009), [http://research.create.usc.edu/cgi/viewcontent.cgi?article=1123&context=nonpublished_reports] (accessed on 27th February 2013);
SMITH, Tony, *Hacker jailed for revenge sewage attacks,* (theregister.co.uk, 2001), [http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/] (accessed on 17th September 2013);
STEADMAN, Ian, *Russian Underground Offers Cybercrime Services at Dirt-Cheap Prices,* (Wired: United Kingdom, 2012), [http://www.wired.com/2012/11/russian-underground-economy/] (accessed 9th July 2014);
STEADMAN, Ian, *The Russian underground economy has democratized cybercrime,* (wired.co.uk, 2012), [http://www.wired.co.uk/news/archive/2012-11/02/russian-cybercrime] (accessed on 21st September 2013);
STEPANOVA, Ekaterina, *Terrorism in asymmetrical conflict: ideological and structural aspects,* (Oxford University Press, 2008), [http://books.sipri.org/files/RR/SIPRIRR23.pdf] (accessed on 24th February 2013);
STROSSEN, Nadine. *Terrorism's Toll on Civil Liberties*, (Haworth Press: USA, 2005;
VICTOROFF, Jeff, *The Mind of the Terrorist: A Review and Critique of Psychological Approaches*, (The Journal of Conflict Resolution - SAGE, 2005), [http://www.jstor.org/discover/10.2307/30045097?uid=3737856&uid=2129&uid=2&uid=70&uid=4&sid=21104625367781] (accessed on 5th May 2013);
WRIGHT, Austin Lee, *Why do terrorists claim credit?* (The University of Texas at Austin, B.A. Government, Sociology: Austin, May 2009), [http://scholar.princeton.edu/austinlw/files/Wright_Paper.pdf] (accessed 14th March 2014);
ZALMAN, Amy, *ETA,* (about.com, 2011), [http://terrorism.about.com/od/groupsleader1/p/ETA.htm] (accessed on 11th May 2011);
ZETTER, Kim, *Future of Cyber Security: What Are the Rules of Engagement?,* (WIRED, 2009), [http://www.wired.com/dualperspectives/article/news/2009/07/dp_security_ars0728] (accessed on 10th August 2012).

AFCEA, *The Russo-Georgian War 2008: The Role of the cyber attacks in the conflict*, (AFCEA, 2012), [http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf] (accessed on 20th March 2013);
AirlineFinancials.com, *How legacy airlines lost so much since 9/11,* (AirlineFinancials.com, 2009), [http://www.airlinefinancials.com/uploads/09_Aug_How_airlines_lost_so_much_altitude_since_9_11.pdf] (accessed on 7th May 2011);
BBC News, *1983: Reagan launches Cold War into space,* (BBC Home: London, 1983), [http://news.bbc.co.uk/onthisday/hi/dates/stories/march/23/newsid_2794000/2794525.stm] (accessed on 15th August 2012);
BBC, *Finland makes broadband a 'legal right'*, (BBC, 2010), [http://www.bbc.co.uk/news/10461048] (accessed on 14th November 2013);

BBC, *Severed cables disrupt internet,* (BBC, 2008), [http://news.bbc.co.uk/2/hi/technology/7218008.stm] (accessed on 13th March 2013);
BBC, *Ship's anchor slows down East African web connection*, (BBC, 2012), [http://www.bbc.co.uk/news/world-africa-17179544] (accessed on 23rd June 2013);
Booz, Allen, Hamilton, *Milestones of Cyber Security,* (Booz, Allen, Hamilton, 2009), [http://www.boozallen.com/media/file/milestones-of-cyber-security.pdf] (accessed on 1st September 2014);
Central Intelligence Agency, *The World Factbook 2013-14,* (CIA: Washington DC, 2013), [https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html] (accessed 12th April 2014);
Cisco Press Release, *Cisco's Visual Networking Index Forecast Projects Nearly Half the World's Population Will Be Connected to the Internet by 2017*, (Cisco: California, 2013), [http://newsroom.cisco.com/release/1197391/] (accessed on 9th June 2013);
CNN Wire Staff, *Obama says U.S. has asked Iran to return drone aircraft,* (cnn.com, 2011), [http://www.cnn.com/2011/12/12/world/meast/iran-us-drone/] (accessed on 5th February 2012);
Committee of Experts on Terrorism, *Federal law no.130 – FZ.,* (Russian Governement, 1998), [http://fas.org/irp/world/russia/docs/law_980725.htm] (accessed on 5th May 2011);
Congress of New Hampshire, *Bill of Rights,* (nh.gov, 2007), [http://www.nh.gov/constitution/billofrights.html] (accessed 21st June 2011);
Continental Congress, *The Declaration of Independence*, (ushistory.org, 1995), [http://www.ushistory.org/declaration/document/] (accessed on 16th May 2011);
Defense Technical Information Centre, *Terrorism*, (Online dictionary of Defense Technical Information Centre, 2011), [http://www.dtic.mil/doctrine/dod_dictionary/data/t/7591.html] (accessed on 5th May 2011);
Department of Defense, *Cyberspace, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011*, (Department of Defense, 2011), [http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf] (accessed on 11th August 2012);
Department of Defense, *Department of Defense Strategy for Operating in Cyber Space*, (Washington DC, 2011), [http://www.defense.gov/news/d20110714cyber.pdf] (accessed on 17th September 2014);
Department of Homeland Security, *National Infrastructure Protection Plan*, (Washington DC, 2006), [http://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf] (accessed on 2nd October 2014);
Department of Homeland Security*, National Srategy to Secure Cyber Space,* (Washington DC, 2003), [https://www.us-cert.gov/sites/default/files/publications/cyber space_strategy.pdf] (accessed on 2nd October 2014);
E.U. Council, *Council Common Position (2001/931/CFSP)*, (E.U. Council, 2001), [http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32001E0931&model=guichett] (accessed on 5th May 2011);
Ericsson, *Analyzing the effect of broadband on GDP,* (Ericsson, 2013), [http://www.ericsson.com/res/thecompany/docs/corporate-responsibility/2013/socioeconomic-effect-of-broadband-speed.pdf] (accessed on 21st February 2014);
Federal Aviation Administration, *Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems,* (FAA, 2009), [http://www.oig.dot.gov/StreamFile?file=/data/pdfdocs/ATC_Web_Report.pdf] (accessed on 15th September 2013);
Federal Bureau of Investigation, *Terrorrism 2002/2005*, (FBI, 2006), [http://www.fbi.gov/stats-services/publications/terrorism-2002-2005/terror02_05.pdf] (accessed on 17th May 2011);
FoxNews, *Chinese hackers took over NASA's Jet Propulsion Lab, Inspector General reveals*, (FoxNews.com, 2012), [http://www.foxnews.com/scitech/2012/03/01/chinese-hackers-nasa-jpl-lab/#ixzz24kilV9N9] (accessed on 10th August 2012);
The Guardian, *Full Text: IRA Statement,* (theguardian.com, 2005), [http://www.theguardian.com/politics/2005/jul/28/northernireland.devolution] (accessed on 5th May 2013);
Israel Foreign Ministry, *The Covenant of the Hamas,* (Israel Foreign Ministry, 1988), [http://www.fas.org/irp/world/para/docs/880818a.htm] (accessed 2nd February 2012);
McAfee, *Global Security Threats and Trends*, (McAfee, 2006), [https://mcafee.imiinc.com/nai7588/aug06/article3.jsp] (accessed on 11th October 2013);

National Cyber Security Centre, *Cyber Security Assessment Netherlands CSAN-3*, (National Cyber Security Centre: Netherlands, 2013), ttps://english.nctv.nl/Images/cybersecurityassessmentnetherlands_tcm92-520108.pdf?cp=92&cs=65035] (accessed 5th May 2014);
National People's Congress, *Decision of the Standing Committee of the National People's Congress on Issues concerning Strengthening Anti-Terrorism Work,* (NPC, 2011), [http://en.pkulaw.cn/display.aspx?id=9082&lib=law] (accessed 11th May 2012);
Net!Works, *Economic impact of the ICT sector*, (Net!Works, 2012), page 5, [http://www.networks-etp.eu/fileadmin/user_upload/Publications/Position_White_Papers/Net_Works_White_Paper_on_economic_impact_final.pdf] (accessed on 18th September 2013);
Norton, *Norton Cybercrime Report,* (Symantec: United States, 2011), [http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/] (accessed 7th June 2013);
Office of Homeland Security, National Strategy for Homeland Security, (Washington DC, The White House, 2002), [http://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf] (accessed on 19th September 2014);
OJR staff, *Post-Mortem: The Bug Appears to Be Beaten,* (USC, 2000), [http://www.ojr.org/ojr/technology/1017966298.php] (accessed on 16th February 2013);
Organization for Economic Co-operation and Development, *Estonia, Review of the Financial System,* (OECD, 2011), [http://www.oecd.org/finance/financial-markets/49497930.pdf] (accessed on 11th October 2013);
President's Office, *National Plan for Infromation Systems Protection*, (Washnigton, The White House, 2000), [http://clinton4.nara.gov/media/pdf/npisp-execsummary-00105.pdf?bcsi_scan_26e330b4cc75177f=0&bcsi_scan_filename=npisp-execsummary-000105.pdf] (accessed on 18th September 2014);
Symantec Press Release, *Top 5 Viruses (*Symantec: United Kingdom, 2013), [http://now.symassets.com/now/en/GB_SITE/pu/images/Promotions/2014/top-5-viruses/images/infographic_TOP_5_Viruses.jpg] (accessed on 9th June 2014);
The Associated Press, *China tech firms pose security risk, U.S. panel warns,* (cbcnews.ca, 2012), [http://www.cbc.ca/news/business/china-tech-firms-pose-security-risk-u-s-panel-warns-1.1286366] (accessed on 21st October 2013);
Tradoc, *US Army, Terrorism and WMD in the Contemporary Operational Environment,* (US Tradoc, 2007), [http://fas.org/irp/threat/terrorism/sup4.pdf] (accessed 21st September 2014);
U.S. Court of Appeals, *USA v. Robert T. Morris,* (U.S. Court of Appeals, 1991), No. 774, Docket 90-1336. [http://www.loundy.com/CASES/US_v_Morris2.html] (accessed on 9th January 2014);
U.S. Government, *National Strategy for Combating Terrorism,* (U.S. Government, 2003) [http://www.upmc-biosecurity.org/website/resources/govt_docs/public_health_prep/whitehouse/whitehouse_national_strategy_for_combating_terrorism.html] (accessed 11th May 2011);
Washington Post, *Timeline: U.S. Government and Cyber Security,* (washingtonpost.com, 2003), [http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html] (accessed on 19th September 2014);
Ynet, *US official: Iran assembled drone like puzzle*, (ynetnews.com, 2011), [http://www.ynetnews.com/articles/0,7340,L-4162745,00.html] (accessed on 5th June 2014).

14.2. Legislative documents

Code of Federal Regulations, (U.S.Government, 2010), [http://www.law.cornell.edu/cfr/text/28/0.85] (accessed on 13th May 2011);
H.R. 145: Computer Security Act of 1987, (Washington DC, Congress, 1987), [https://epic.org/crypto/csa/csa.html] (accessed on 16th September 2014);
H.R. 3162: USA Patriot Act, (Washington DC, Congress, 2001), [https://epic.org/privacy/terrorism/hr3162.html] (accessed on 16th September 2014);
H.R. 3394: Cyber Security Research and Education Act of 2002, (Washington DC, Congress, 2002), [http://csrc.nist.gov/drivers/documents/HR3394-final.pdf] (accessed on 16th September 2014);
H.R. 3523: Cyber Intelligence Sharing and Protection Act of 2011, (Washington DC, Congress, 2011), [http://www.gpo.gov/fdsys/pkg/BILLS-112hr3523ih/pdf/BILLS-112hr3523ih.pdf] (accessed on 16th September 2014);
H.R. 5005: Homeland Security Act of 2002, (Washington DC, Congress, 2002), [https://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf] (accessed on 16th September 2014);

H.R.3524: Computer Network Protection Act of 1989, (Washington DC, Congress, 1989), [http://thomas.loc.gov/cgi-bin/query/z?c101:H.R.3524.IH:] (accessed on 16th September 2014);
H.R.4922: Communications Assitance for Law Enforcement Act, (Washington DC, Congress, 1994), [http://www.gpo.gov/fdsys/pkg/BILLS-103hr4922rds/pdf/BILLS-103hr4922rds.pdf] (accessed on 15th September 2014);
S.1766 – Federal Computer Systems Protection Act, (Washington DC, Congress, 1977), [http://www.gao.gov/assets/100/98793.pdf] (accessed 27th October 2014);
U.S. Code, (U.S. Government), [http://www.law.cornell.edu/uscode/text/18/16] (accessed on 21st January 2012).

14.3. Web pages

"1st IO Command," official web pages of this unit, http://www.1stiocmd.army.mil/ (accessed on 8th August 2012);
"67th Network Warfare Wing," official web pages of this unit, http://www.24af.af.mil/units/67nww.asp (accessed on 5th August 2012);
"688th Information Operations Wing," official web pages of this unit, http://www.688iow.af.mil/ (accessed on 6th August 2012);
"689th Combat Communications Wing," official web pages of this unit, http://www.24af.af.mil/units/689ccw/index.asp (accessed on 7th August 2012);
"Army Cyber," U.S. Army Cyber Command official web pages, http://www.arcyber.army.mil/org-uscc.html (accessed on 7th August 2012);
"Naval Network Warfare Command," official web pages of this unit, http://www.netwarcom.navy.mil/ (accessed on 7th August 2012);
"Oxford Dictionary", Oxford Dictionaries, [http://oxforddictionaries.com/] (accessed on 21st January 2012)
"United States Army Intelligence and Security Command," official web pages of this unit, http://www.inscom.army.mil/ (accessed on 8th August 2012);
"Communications - the Future is Now", Hong Kong Polytechnic University, http://www.alanptlau.com/Research.html (accessed on 2nd July 2013);
"DOD Releases Fiscal 2013 Budget Proposal," Department of Defense official web pages, http://www.defense.gov/releases/release.aspx?releaseid=15056 (accessed on 2nd August 2012);
"Foreign Terrorist Organizations", official site of the U.S. Department of State, http://www.state.gov/j/ct/rls/other/des/123085.htm (accessed 28th April 2014);
"Internet World Stats 2012" , Internet and world stats – usage and population statistics, http://www.internetworldstats.com/stats.htm (accessed on 3rd April 2013);
"Key ICT indicators for developed and developing countries and the world (totals and penetration rates)", ITU World Telecommunication/ICT Indicators database, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/ITU_Key_2005-2014_ICT_data.xls (accessed on 6th May 2014);
"Layering in Networked Computing", Goldsmiths Department of Computing, University of London, http://doc.gold.ac.uk/~mas01lo/Teaching/cis110/sem2/lectures/ppt/layering.ppt (accessed on 27th September 2013);
"Nupedia", Wikipedia, http://en.wikipedia.org/wiki/Nupedia (accessed on 13th January 2012);
"Our Mission", Official site of the Department of Homeland Security, http://www.dhs.gov/our-mission (accessed on 28th September 2014);
"The leader in global business communications", Global Cloud Xchange, http://www.relianceglobalcom.com/about-us.html (accessed on 26th August 2013);
"Wikipedia", Wikipedia, http://en.wikipedia.org/wiki/Wikipedia (accessed on 13th January 2012).

14.4. Database

National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2013). Global Terrorism Database [Data file]. Retrieved from [http://www.start.umd.edu/GRD]

14.5. Conference contributions

Alexander Klimburg, research fellow at Belfer Center for Science and International Affairs, Cambridge/US, *Prague Transatlantic Talks 2014: Facing the Atlantic Cyber Challenge Conference* (Prague, 28th – 29th May 2014), mentioned during open discussion;

Tom Fastner, a Senior Member of the Technical Staff and an Architect with eBay, Teradata CTO Roadshow (Silicon Valley, 23rd June 2014), presentation on Teradata solution for eBay.

14.6. Software

Gnu Regression, Econometrics and Time-series Library (GRETL), downloaded from [http://gretl.sourceforge.net/#dl], open license;
Testy nahodnosti (TestRand), downloaded from [http://thanzak.sweb.cz/Download.htm], open license;
SAS learaning edition 4.1., student's license.