ELECTRONIC GOVERNMENT IN THE FIGHT AGAINST TERRORISM

Žaklina Spalević[1],
Miloš Ilić[2*],
Željko Spalević[3]

[1]Singidunum University,
Belgrade, Serbia
[2]University of Pristina,
Faculty of Technical Science,
Kosovska Mitrovica, Serbia
[3]University Donja Gorica,
Podgorica, Montenegro

Abstract:
Electronic government provides different interactions between government and citizens, government agencies, employees and businesses or commerce. All these interactions provide better, faster and safer use of government services. In today's world, electronic government services have one very important role and that is war against terrorism. In this context, terrorism implies traditional and cyber terrorism. Network connections between different government services, use of databases with registered terrorists and terrorist organizations, electronic monitoring and checking of individual on the borders or suspicious web sites can prevent future attacks. This paper summarizes and presents different use of government electronic service in the war against terrorism through technical and legal observation. Besides advantages and disadvantages of the current electronic services, the paper presents ideas for possible improvements and better law support.

Key words:
electronic monitoring, cyber-crime,
terrorist activity activity, border control.

Acknowledgment
This work has been supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia within the projects TR 32023 and TR 35026.

1. INTRODUCTION

Electronic government is being increasingly recognized as a means for transforming public governance. E-government is also known by different terms such as Electronic Government, Electronic Governance, Digital Government, Online Government, e-Gov *etc.* (Gronlund and Horan, 2005). In fact, there are many definitions for the term e-Government and their differences reflect the priorities in the government strategies. Some authors define e-government as a way for governments to use the most innovative information and communication technologies, particularly web-based Internet applications, to provide citizens and businesses with more convenient access to government information and services, to improve the quality of services and to provide greater opportunities to participate in democratic institutions and processes (Fang, 2002). Another definition of e-government is as the government owned or operated systems of information and communication technologies that transform

Correspondence:
Miloš Ilić

e-mail:
milos.ilic@pr.ac.rs

DOI: 10.15308/Sinteza-2016-518-525

relations with citizens, the private sector and/or other government agencies so as to promote citizens' empowerment, improve service delivery, strengthen accountability, increase transparency, or improve government efficiency. E-government offers services to those within its authority to transact electronically with the government. These services differ according to users' needs, and this diversity has given rise to the development of different type of e-government. E-government functions can be classified into four main categories: Government-to-citizen (G2C), Government-to-business (G2B), Government-to-government (G2G), Government-to-employee (G2E).

E-government has potential for stronger institutional capacity building, for better service delivery to citizens and business, for reducing corruption by increasing transparency and social control (DPEPA, 2002). Measuring the return on e-government investments recommends that any successful e-government program should address at least one of the following areas: financial – reduced costs of government operations with enhanced revenue collection; economic development; reduced redundancy - consolidating and integrating government systems; fostering democratic principles; and improved service to citizens and other constituencies. E-government should enable anyone visiting a city website to communicate and interact with city employees via the Internet with instant-messaging (IM), audio/video presentations, and graphical user interfaces (GUI). This needs to be more sophisticated than a simple email letter to the address provided at the site. Technology was used to improve the access to website, and delivery of government services. Data collected and shared through these kinds of services can be used for many different purposes.

Besides citizens and companies, employees in the government services use these data to apply security measures to secure homeland, government and their citizens from traditional and cyber terrorist attacks. In case of traditional terrorist attacks, police authorities in the country and cross border control could monitor suspicious persons and prevent attacks, relying on the information collected about previous terrorist activity, and the data collected from biometric documents. Also, network of cellphones can be used to track individuals, their locations and conversations. Cyber terrorism must be considered to include the full range of threats, vulnerabilities, risks and technological matters. That could be the use of computer network tools to harm or shut down crucial national infrastructures. By this, energy, transportation and government operations are meant. The premise of cyber terrorism is that as nations and critical infrastructure become more dependent on computer networks for their operation, new vulnerabilities are created (Weimann, 2004). The definition of cyber terrorism has been highly debated since the 1990s, because it is not easy to define how devastating the damage caused by a single computer attack might be. The term itself has been controversial, sometimes inflated and used in different contexts. Today, monitoring of users who visit critical web sites which are considered to be the property of terrorists may lead to useful information. What drives people to terrorism is not easy to determine.

One thing is for sure, the terrorists are not willing to be observed in their activities. Such observation could provide appropriate information and conclusions. To prevent attacks from different terrorist organizations, government agencies must contain appropriate information and good cooperation between themselves. The main goal of this paper is to make the readers conversant with the role of e-government services in the war against terrorism. In continuation, different mechanisms for terrorist monitoring and information collections are presented. One part of the paper underlines their benefits and shortcomings, and the other presents technical solutions and law regulations for improvements for those mechanisms.

2. BIOMETRIC DOCUMENTS

National Identification Documents or eID programs are implemented in many countries by issuance of identity cards to citizens. Stealing someone's identity is a big intrusion of the privacy with major consequences on the legal and financial transactions.. In many cases, stolen ID cards are used for criminal activities. Identity cards can be extended with biometrics data about the user to ensure a unique ID and to prevent identity fraud. Biometric technologies provide protection of multiple registrations by the same person. Different biometric documents are used for different purposes. Each of those documents has specific architecture, and uses some kind of biometrics. Different government services require from citizens to own and use different biometric documents in different situations. Biometrics and security mechanism in biometric documents will be presented on the example of e-passports.

The e-passport contains an RFID chip which holds sensitive information: passport number, issue and expiry

date, issuing country, full name, gender, nationality, date of birth, document type, digital picture of the passport holder, and fingerprint or iris scans. Radio Frequency Identification (RFID) is an automatic identification technology that transmits data through the use of wireless communication using radio waves. An RFID system for e-passport consists of a chip, a reader, an antenna, and a Public Key Infrastructure (PKI).

The international agreements on electronic documents such as passports require a biometric identifier, which is used to verify that the person presenting the passport is really its owner. Biometric parts in electronic passport are digital version of the facial photograph and fingerprints. Facial photograph of an applicant is employed as a basic security element. From a biometric point of view, the face contains information that is invariant in time and can be measured, for example, the distance between eyes, position of chin, position of nose, and so forth. For the purpose of picture data creation, government agency responsible for passport creation must behave and take picture according to the specifications in ISO19794-5 that defines conditions for acquirement of this type of data: format, scene, picture properties, and so forth (Malčík and Drahanský, 2012). Organization of passport chip memory provides appropriate possibility for picture data storage twice on the chip. A chip consists of sixteen memory parts named data group one to data group sixteen respectively. The first copy of picture is encoded and stored in *data group two,* which is predefined for facial photograph in full color.

The second picture copy is stored in so called *data group five* on the chip. This picture is gray scale, and it is designated for laser engraving.

Another important biometric attribute stored on the biometric document's chip is fingerprint. That is an attribute that has been studied intensively. The fingerprint represents the unique skin structure of fingertips. As a phenotypic biological feature, fingerprint is unique, even in the case of identical twins. The characteristic formation of the fingerprint normally doesn't change over a person's life span (Schimke *et al*, 2005). Most fingerprint recognition systems analyze the unique pattern of ridges and valleys, and the arrangement of small unique marks on the fingerprint, which are known as minutiae. They can be recognized and distinguished by their type, by x- and y-coordinates, and by their direction. For storage of complete fingerprint image data on the biometric document's chip, up to 250 Kbytes is needed. Using different compressions, size of data can be reduced. By saving only extracted information, a reduction to a magnitude of one Kbyte is possible. This can provide the lack of interoperability between biometric systems from different vendors, if these systems use different types of feature data. To avoid fake-finger attacks, some systems employ so-called liveness detection technology, which takes advantage of the sweat activity of human bodies. High-magnification lenses and special illumination technologies capture the finger's perspiration and pronounce the finger dead or alive. To provide more safety for their citizens, all EU countries are working to add fingerprint biometrics protected to the e-passport, and are currently conducting cross-border tests of these more advanced e-passports. For instance, Germany has two fingerprints, one from each hand, in the country's passport.

Registered attacks and vulnerabilities

While a biometric system can be compromised in a number of ways, one of the potentially damaging attacks is the leakage of biometric template information. The leakage of this template information to unauthorized individuals constitutes a serious security and privacy threat. If an attacker can hack into a biometric database he can easily obtain the stored biometric information of a user. This information can be used to gain unauthorized access to the system by either reverse engineering the template to create a physical spoof or replaying the stolen template (Jain *et al*, 2013). The attack can take place at communication network, chip or at backend system. E-passport guarantees confidentiality, consistency and authenticity of information based on some cryptographic tools, but it is not fully protected. The most common hardware and software attacks include the following:

- Eavesdropping. This is an attack where the attacker intercepts the information by using an unauthorized device during the communication between a chip on the passport and legitimate reader. This is mainly due to the fact that e-passports use the communication network of RFID cards (Pooters, 2008). Eavesdropping can result in stolen sensitive information, such as e-passports biometrics, personal information or cryptography information.
- Clandestine Scanning and Tracking. It is well known that RFID tags are subject to clandestine scanning. Baseline International Civil Aviation Organization (ICAO) guidelines do not require

authenticated or encrypted communications between passports and readers. Consequently, an unprotected e-passport chip is subject to short-range clandestine scanning (up to a few feet), with attendant leakage of sensitive personal information including date of birth and place of birth. The standard for e-passport RFID chips (ISO 14443) stipulates the emission of a chip ID on protocol initiation (Sheetal, 2006). If this ID is different for every passport, it could enable tracking the movements of the passport holder by unauthorized parties. Tracking is possible even if the data on the chip cannot be read.

- Cloning. This is copying or duplicating data of a chip found in the Machine Readable Zone (MRZ) to another chip or system without the knowledge of the passport holder. This type of attack occurs to the mandatory feature of passive authentication. Many researchers have identified that cloning is a serious vulnerability and successful attacks can compromise confidentiality of the MRZ e-passport chip data (Sinha, 2011). The cloning poses a threat of data and biometrics leakage contained in the e-passport chip. Besides leakage of biometric data, alteration of biometric data is possible (Nithyanand, 2009).
- Cryptographic Weaknesses. Many services which use e-passports include an optional mechanism for authenticating and encrypting passport-to-reader communications. The idea is that a reader initially makes optical contact with a passport, and scans the name, date of birth, and passport number to derive a cryptographic key K with two functions: it allows the passport to establish that it is talking to a legitimate reader before releasing RFID tag information, and it is used to encrypt all data transmitted between the passport and the reader (Juels *et al*, 2005). Once the reader knows the key K, however, there is no mechanism for revoking access.
- Skimming. A skimming is the act of obtaining encoded data without the consent of users by using electronic storage device. Moreover, the RFID e-passport chips transmit radio waves broadcasting information once the e-passport is either partially or fully open, which makes the e-passports prone to skimming (Sheetal, 2006). The data from e-passport can be retrieved by beaming power at the passport within a few inches or at most a few feet.

Improvement in the use of biometric documents

Biometric documents in different government institutions provide the appropriate citizen identification. To prevent previously numbered attacks and vulnerabilities, each country tries to develop more secure biometric documents. One way to improve this kind of documents is to put more biometric data about the person on the document's chip.

For example, in addition to fingerprint and face photo, scanned iris structure could be placed on the biometric document's chip. The biggest advantage of iris scanning is its accuracy and reliability. Iris scanning is ten times more accurate than fingerprinting. Some research have shown that iris scanning produces around 1 in 1–2 million false matches, compared to fingerprints, which produce around 1 in 100,000. While fingertips are constantly susceptible to damage, the iris in the other hand is naturally protected by the cornea. Iris pattern seems to remain reliably unchanged for decades. Unlike fingerprint scanners, which need direct contact and have to be kept spotlessly clean, iris scans can be performed safely at some distance from the eye.

More biometric data on one document provide better security. Today's government services around the world work to create dual-biometric documents. These documents use different combinations of biometric data in the process of identity verification. One research example combines dual-iris recognition and face capture capabilities. This kind of biometric protection which uses multiple biometric factors is a new solution for biometric documents creation (Counter, 2014). The big deal about this deployment solution is the new technology which uses iris scanning and recognition. This iris recognition system is developed for everyday practical use in real life. Biometric scanners used for this kind of job provide precise iris scanning from a distance. Those scanners do not require from the subjects to stop moving their eyes.

Another dual or multimodal biometric system proposes dual-biometric-modality personal identification, which used both the fingerprint and the Electroencephalogram (EEG) technologies to achieve both high identification performance, and an effective antispoofing capability (Liwen *et al*, 2010). That study represents the first effort to fuse the widely adopted fingerprint technology with a novel biometric modality-EEG. Experimental results suggest that the highest identification performance is obtained in the proposed dual-biometric modality system, compared with the performance of the systems based on either fingerprint or EEG alone.

Different studies about dual-biometric personal documents suggest using different biometric data. All biometric documents provide quite enough data for successful control by government services. Retention time of the people who cross the border is very important. Because of that, frontiersman must… triage suspicious of not suspicious persons. A system which compares citizen's data from the biometric document with data from government database about citizen must work fast as much as possible. If data about some person are suspicious, additional checks must be done. In such situations, biometric data from the document would be checked. If the document is stolen or data altered, matching will not be possible. In order to provide better control, governments must develop and use automated control systems. While personnel do the passport or ID check of the person, automated system for face recognition could compare picture collected from the camera on the border, and one from the document. If there is no match of the pictures, or picture and personal data (name, last name, address…), fingerprint or iris scanning could be done for additional check.

An example from USA shows that the man arrived to New York's John F. Kennedy International Airport and presented a valid passport and a visa (Homeland, 2015). The name and picture on his travel documents were appropriate, but the fingerprints check revealed that he was trying to use the visa which belongs to his twin brother, who had no prior criminal recod or immigration violations. By matching his biometrics, officers found out that this man had been arrested for taking photos of a U.S. military base. Besides that, he had extended the term of his admission on a previous visit to the United States. This and other examples show that the use of a large number of biometric characteristics leads to greater safety, and could provide higher protection against terrorism.

3. GLOBAL NETWORKS AND TERRORISM

Most terrorist groups are now leveraging the Internet to recruit, train and spread propaganda, especially "global brands" such as al-Qaeda. Criminal groups and foreign intelligence services appear to have demonstrated electronic theft and sabotage capabilities. All terrorist groups and individuals find the Internet useful. Today, almost each terrorist organization has websites, and many of them have more than one website created in several different languages (Winder, 2014). Terrorist websites make use of slogans and offer items for sale, including videotapes, audiocassettes, t-shirts, badges, and flags. All things are offered in order of sympathizing. Terrorist organization will target local supporters through the website in the local language, and will provide detailed information about the activities, politics of the organization, its allies, and its competitors. Terrorist organizations use the Internet in many different ways. Some of those examples include the following:

- Networking and information sharing: The Internet is overcrowded with information that could be used by terrorist groups. Such groups could find different maps, satellite area photos and plans. Besides that, terrorists can use the Internet to find information about communication and transportation infrastructure, water supplies systems, explosives manufacturing, creation of fraudulent passports, and information about different weapons. Terrorist groups share different kinds of information among themselves. They share news events, publishing manifestoes, or logistic and tactical information. In most cases, they are relying on password protected forums, chat rooms and bulletin boards. Lately, a number of large-scale terrorist groups have become less centralized and more extensively networked. They use social networks for communication, and fun group creation.
- Recruitment: In the case of terrorism, recruiting new activists is very important. In many cases, political and/or religious rhetoric is used for this job. Marketing and propaganda are oriented towards young adults, because of the fact that young adults are the most abundant internet users. Because of their age, they are consequently among the most predisposed to propaganda.
- Fundraising: Websites for terrorist organizations often have links which redirect the visitors to another address on which visitors are often monitored and researched. Visitors who visit website over and over and those who stay on the website for longer periods of time will be contacted. They will be offered additional information or asked for assistance.
- Cyberterrorism: It is focused on hacking or cracking into victims computers for the purpose of disruption, privacy data disclosure or misuse. Potential targets are telecommunication systems, defense systems, medical facilities, power grids, transportation, and public persons and politicians.

Terrorist websites and social networks tracking and control

In response to the growing number of extremist websites and social networking sites, government agencies have started to carry out cyber vigilantism. Because of the nature of the counter-terrorism, the government does not provide exactly what technology is being used for. Information on how some cyber protection is being implemented is not in the public domain. However, it is obvious that communication monitoring techniques are at the very heart of the surveillance and interception policy. How terrorists communicate, of course, is also a big problem for the government. One method in the fight against terrorist websites, and terrorist activity on the social networks is website tracing and blocking by government agencies. The authors shall present the examples of different foreign practices.

In an attempt to proactively defend against web based terrorist's tactics, the Metropolitan Police in the UK established a dedicated Counter Terrorism Internet Referral Unit (CTIRU) in 2010 that deals with public reports of online content of a violent extremist or terrorism nature. Since it started, CTIRU has removed some 55,000 pieces of content and 34,000 of those have been in the last year alone. More controversially, the UK government is putting pressure on the Internet service providers to block extremist content at source, so that customers would not be able to see it. This blocking would, if successful, take the form of optional filtering such as is already in place for pornographic content.

A new legal decree that went into effect in February 2015 allows the French government to block websites accused of promoting terrorism and publishing child pornography, without seeking a court order (Toor, 2015). Under the new rules, the Internet service providers must take down offending websites within 24 hours from receiving a government order. The decree implements two provisions from two laws: an anti-child pornography law passed in 2011 and an anti-terror law. According to the law, the department of the French national police is responsible for identifying the sites to be blocked, with the suspected terror-related sites subject to review by an anti-terrorism branch. Once the site is blocked, its page will be replaced with an explanation of why the government took it down.

In 2003, FBI agency decided to explore developing a web application that would monitor user updates on social sites such as Facebook and Twitter for the purpose of tracking possible terrorist activities on social networks (Teeter, 2003). The application is developed so the FBI could quickly vet, identify, and geo-locate breaking events, incidents and emerging threats. FBI agents employed in the communications center, sending out real-time alerts, developing threat profiles and detecting potential threats to the field agents. American people are willing to sacrifice some of their on-line privacy if it helps in the fight against terrorism: 57% of both Americans and Internet users agree that Internet users should be willing to give up some privacy if it helps law enforcement officials to track down terrorists (Jongman, 2011). Thirty-nine percent of both groups disagree, however, saying that the terrorists would ultimately win if people lost any of their civil liberties.

One more technique in the fight against terrorist activities in the cyber space is monitoring of suspicious websites and social networks profiles. Through social networks, government agencies could monitor and cluster all users who walk into any suspicious activity. By this we refer to social network users who frequently comment, like and visit terrorist fan page. The most frequent and active (support comments) visitor can be put on the so called terrorism watch list. Technically, that is the database with all possible information about such user. This kind of databases shared among different government agencies could prevent future terrorist attacks. For example, if the citizen whose name is in some kind of database will be more carefully controlled on the border, or in some important public institutions. In some cases, border crossing or airplane travel will be forbidden.

United States created Terrorist Screening Database (TSDB). If the person is a known terrorist or if there is a reasonable suspicion that the person could be terrorist, it will be included in this database (TSC, 2015). To meet the reasonable suspicion standard, nominating agencies must rely upon articulable intelligence or information which reasonably warrants a determination that an individual is suspected to be a potential terrorist (TSC, 2015). Based on the totality of the circumstances, a nominating agency must provide an objective evidence to believe an individual is a known or suspected terrorist. Nominations to the TSDB are not accepted if they are based on ethnicity, race, religious affiliation, and national origin. Activity such as the exercise of religion, free speech, freedom of the press and freedom of peaceful assembly are protected from nomination for TSDB by First Amendment.

Each person who has some problem with control on the airports or borders could check if his/her name is on some watch list. There is a process called the Department

of Homeland Security Traveler Redress Inquiry Program. This is program which allows a person to make an inquiry if their name is on the list, and why their name is on it. The program rescans person's name and then, if person was wrongly put on the list, they will remove his/her name from the list, but that is not a simple process. For example, if a person have trouble at the airport, that person should contact the Transportation Security Administration and complete the paperwork for redress program. Paperwork will be passed to the authorities that evaluate any necessary changes. The average wait time for resolving a complaint is sixty-seven days (DoJ, 2007). With so many people being identified as possible terrorists, it may seem nearly impossible for a watch-listed person to slip through government screening. However, an audit by the U.S. Department of Justice in 2007 found that twenty people who were on the watch list were not properly identified and detained when they should have been (DoJ, 2007). In many cases, complains are being rejected, and the person being moved on the hider level of protection. In some cases, person being moved on the lower level, but still stay on the watch list.

4. CONCLUSION

Homeland security of each country depends on many facts. Domestic and foreign enemies and terrorists seek a way to comprimise or jeopardise the security of citizens. In order to provide appropriate security level for all citizens government agencies all over the world work to find the best solution in the fight against terrorism. Because of the huge number of possible terrorist methods, agencies must work together in this fight. The one described above are biometric documents, which provide citizen's information transparency to agencies. Although hardly accepted, these documents offer different possibilities to their users. Some of them are digital signatures and digital certification. All those possibilities and basic biometric information from another hand are important for successful citizen protection.

Network connections between government agencies provide faster information sharing. This is important because of the fact that different agencies could have the same information about some possible terrorist activity at the same time. Cyber terrorism and terrorist activities on the Internet are monitored by appropriate government agencies. As we have explained and presented through the examples, finding, monitoring and blocking of terrorist web sites and social networks profiles are three most important activities. This order between mentioned activities is selected because firstly, it is important to find and mark possible terrorist web site, fan page or user profile. After that and before web site blocking, agencies must collect all important information about the web site owner and visitor through the monitoring process. This kind of information could put some internet user on the terrorist watch list. At the end, web site will be blocked. Internet service providers are responsible for this job by the government order.

Each country has legal directives which provide instruction that must be fulfilled in order to prevent terrorism. Law against terrorism is different in different countries, but targets the same ideas. This law defines rights and obligations of government agencies and defines in which situations some person or organization could be marked as a terrorist threat. Our final conclusion is that in the fight against terrorist threats all government institutions must work together in order for the success to be evident.

REFERENCES

Counter, P. (06.01.2014). *The Biometric Upgrade: SRI International Introduces IOM PassPort SL.* Retrieved 25.02.2016, from http://findbiometrics.com/the-biometric-upgrade-sri-international-introduces-iom-passport-sl/

DoJ (U.S. Department of Justice) (2007). Follow-Up Audit Of The Terrorist Screening Center, Office of the Inspector General Audit Division, U.S.

Fang, Z. (2002). E-government in digital era: concept, practice, and development. *International journal of the Computer, the Internet and management*, 10(2), 1-22.

Gronlund, A., & Horan, T. A. (2005). Introducing e-gov: history, definitions, and issues. *Communications of the association for information systems*, 15(1), 713-739.

Homeland Security (2015).*Enhancing Security Through Biometric Identification.* Retrieved 01.03.2016, from https://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_biometrics_brochure_english.pdf

Jain, A. K., Nandakumar, K., & Nagar, A. (2013). Fingerprint template protection: From theory to practice. In Security and Privacy in Biometrics (pp. 187-214). London: Springer London.

Jongman, B. (2011). Internet Websites and Links for (Counter-) Terrorism Research. *Perspectives on Terrorism*, 5(1).Chicago.

Juels, A., Molnar, D., & Wagner, D. (2005). Security and Privacy Issues in E-passports. *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on* (pp. 74-88). IEEE.

Liwen, F. S., Cai, X. A., & Ma, J. (2010). A dual-biometric-modality identification system based on fingerprint and EEG. In Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on (pp. 1-6). IEEE.Chicago.

Malčík, D., & Drahanský, M. (2012). Anatomy of biometric passports. *BioMed Research International*, *2012*,1-9.

Nithyanand, R. (2009). A Survey on the Evolution of Cryptographic Protocols in ePassports. *IACR Cryptology ePrint Archive*, 2000(200).

Pooters, I. (2008). Keep Out of My Passport: Access Control Mechanisms in E-passports. Retrieved January 18. 2016, from https://danishbiometrics.files.wordpress.com/2010/ 05/ ivo.pdf.

Schimke, S., Kiltz, S., Vielhauer, C., & Kalker, T. (2005). Security analysis for biometric data in ID documents. Proceedings of the Security, Steganography, and Watermarking of Multimedia Contents VII, 2005 (pp.474-485). San Jose, Ca, USA. - S.l: Technische Universiteit Eindhoven.

Sheetal, S. (2006). Technical analysis of security mechanisms used in RFID E-passport, related threats, security and privacy issues. *Viterbi School of Engineering, University of Southern California*.

Sinha, A. (2011). A Survey of System Security in Contactless Electronic Passports. *International Journal of Critical Infrastructure Protection,* 4(3), 154-164.

Teeter, H. (2003). E-Government: To Connect, Protect and Serve Us. 1724 Connecticut Avenue, NW Washington, D.C. 20009.

Toor, A. (09.02.2015). *France can now block suspected terrorism websites without a court order.* Retrived 20.01.2016, from http://www.theverge.com/2015/2/9/8003907/france-terrorist-child-pornography-website-law-censorship

TSC (25.09.2015). *Terrorist screening center*, Federal Bureau of Investigation, Retrived 20.02.2016, from https://www.fbi.gov/about-us/nsb/tsc/

United Nations Division for Public Economics and Public Administration, (2002). *Benchmarking E-Government: A Global Perspective-Assessing the Progress of the UN Member States*. Retrieved February 12. 2016, from https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/English.pdf.

Weimann, G. (2004). Cyberterrorism, How Real Is the Threat?. *United States Institute For Peace*, 1-12.

Winder, D. (09.12.2014). *Anti-terror measures: How tech helps fight the counter-terrorism war.* Retrived 20.02.2016, from http://www.itpro.co.uk/security/23685/anti-terror-measures-how-tech-helps-fight-the-counter-terrorism-war