DARK WEB, CYBER TERRORISM AND CYBER WARFARE: DARK SIDE OF THE CYBERSPACE

Vida M. VILIĆ
PhD, Clinic of Dentistry Niš, Assistant Director for Legal Matters,
e-mail: vila979@gmail.com

Abstract

Cyberspace allows much easier access for a greater number of people, especially young people, to the propaganda of terrorist organizations and illegal activities. This kind of communication and dissemination of terrorist and criminal ideas is not only much cheaper, because it requires only an investment in a computer and access to the network, but it is anonymous, it is not spatially limited, terroristic idea and terroristic actions are performed at the same time, while the consequences can affect even more people and targets than is the case of "offline" criminality and terrorism. In recent years, the increasing problem that experts talk of in public is the "dark side of surfing the internet", the "Dark net" or the “Deep Web".

Cyber terrorism is a modern form of terrorism, which connects the virtual space and terrorist activity, by manipulating even more efficient methods of psychological warfare. In the cyberspace you never know who could be the next victim. Based on the characteristics of cyber terrorism and cyber warfare, it is possible to reconstruct the criminological dimensions of the terrorist attacks in cyberspace. Social networks can be used by terrorists for the purpose of psychological warfare in order to spread disinformation, fear, panic, intimidating messages and threats to the public.

Since there is not a unique definition of cyber terrorism, this paper presents various definitions, implying numerous characteristics of this kind of criminal activity. The paper also pointed out to some of the international legislation that made great efforts in order to effectively counter fight cyber terrorism, both on international as well as at member state level, and emphasized the need for interstate and intergovernmental cooperation on three parallel levels: through international organizations, through multilateral and multinational platforms and through regional action.

Keywords: *cyberspace, cyber terrorism, cyber warfare, steganography, encryption, social networks, international legislation*

Introduction

Even though the benefits of the Internet in modern society are numerous, the same technology which facilitates modern life can also be exploited by terrorists and terrorist organizations. Cyberspace can also be the perfect place for the glorification of terrorist acts, motivation for committing the acts of terrorism, recruitment of terrorists, broadcasting the illegal and violent content, facilitating communication between terrorists and terrorist groups and the training of potential recruits, just like in real life only easier, with anonymity and much cheaper.

In recent years, an increasing problem that experts talk in public is the dark side of surfing the internet, Dark Net, Dark Web or Deep Web, where data and information are password locked, trapped behind pay walls, or where the user is required to use special software to access this data. It is estimated that this "digital underground" is much bigger than the regular internet and that hackers, criminals, terrorists or pedophiles can carry out their illegal activities with complete freedom. Deep web is part of the internet that is not accessible to regular browsing tools or to everyday browsing methods. It is a part of the cyberspace based on standard services and protocols, but requiring specific identification for use: they are completely legal but not public services. Dark Web, or Dark Net, is a part of the Internet which is also not accessible to regular browsing tools or to everyday browsing methods, but it requires special skills or data in order to connect the various illegal activities in cyberspace. Dark Web is the "promised land" for users who want to buy and sell drugs, counterfeit money or forged documents, weapons, ammunition or explosives, to order and pay for someone's murder, or to obtain human organs (Anonimus, 2015). Dark Web has a special system of online payments concealing identity. Considering that illegal activities on the Dark Web and cyber terrorism are new areas of possible computer and network misuse and criminality, comprehensive theoretical and empirical research on this phenomenon is still in development.

What is cyber terrorism?

Cyber terrorism is a modern form of terrorism, which connects two greatest fears of modern times: the virtual cyberspace and terrorist activity, which refers to "unlawful attacks and threats of attack against computers, networks, and the information stored therein" in order to "intimidate or coerce a government or its people in furtherance of political or social objectives" (Manap., N.A., & Tehrani, P.M., 2012: 409). Internet space is very suitable

for various terrorist activities and operations, as it provides a facility for secure communications with a very low cost (Ranđelović, D., Bajagić, M., & Carević, B., 2012: 318). Cyberterrorism, as a part of the cyberwarfare,[1] refers to deliberate, politically motivated attacks on computer systems and programs, as well as spreading the data which could provoke violence and fear with the civilian targets, in order to persuade the government to change its policy (Gaćinović, R., 2012:15). Both cyber terrorism and cyber warfare have the same characteristics: the similarity of their goals, almost the same manner of execution (modus operandi), but they differ a bit in the strategy of planning, perpetrators, and potential targets. Cyber warfare has largely been the province of nation states, and it is generally believed by cyber security experts that wide-scale cyber warfare can be conducted only by national actors, mostly by state sponsorship. The real question, according to Stewart (2015) is "Can an enemy employs asymmetrical warfare in the cyber realm"? The new weapon in virtual wars that are used are Logic Bombs, Troyan horses, Worms and Viruses.[2] Its main objectives are: to disable the system from functioning properly with the loss of information, to use different software to overload telephone and internet networks, air force control and to control computers responsible for supervision of other forms of transport, to scramble or misuse programs that large institutions from state significance and emergency services use.

There is no unique and universally accepted definition of cyber terrorism, but all given definitions point out that some of the elements of this criminal activity include: data theft or hacking, planning terrorist attacks, causing violence, attacks on information systems and computer networks. However, internet terrorism must be considered separately from computer crime in general, because every attack on a computer or network system does

[1]Cyberwarfare can be defined as "any virtual conflict initiated as a politically motivated attack on an enemy's computer and information systems" which "disable financial and organizational systems by stealing or altering classified data to undermine networks, websites and services", and it is also known as cyber warfare or cyber war. *See:* Techopedia, https://www.techopedia.com/definition/13600/cyberwarfare.

[2]Viruses are malicious software that attach themselves to legitimate looking program or file in order to cause damage. A worm is a malicious program that can replicate itself onto other computers on a network. A trojan horse is a malicious program that can be used to for accessing data, erasing files, stealing passwords. Logic bombs are usually pieces of code that are programmed into a program that lie dormant until a certain
time or until a user does a certain action which causes it to be executed. *See:* Hack Defence, http://hackdefencesecurity.blogspot.rs/2012/02/1.html

not necessarily represent the act of cyber terrorism. If the cyber terrorism is equated with daily attacks on computer and network systems, it would be an even bigger problem to determine with certainty the identity, intention or political underpinning of the perpetrator, because most of the cyber perpetrators are hiding behind their anonymity in cyberspace and false IP addresses. For this reason, cyber terrorism is properly defined as "politically motivated use of computers as weapons or as targets, by sub-national groups or clandestine agents intent on violence, to influence an audience or cause a government to change its policies" (Wilson, C., 2005: 5-7).

The term "cyber terrorism" was used for the first time in the 1980s by Barry C. Collin of the Institute for Security and Intelligence, who discussed this dynamic of terrorism as transcendence from the physical to the virtual realm and "the convergence of these two worlds", which "move ahead with blinding speed into the computerization of every task and process that we face" (Collin, C. B., *n.d.*).

Some authors, such as James A. Lewis (2002:1), define cyber terrorism as "the use of cyber computer networks and internet tools for breaking critical national infrastructures (such as energy, public transport, government activities) or to intimidate or compel a government of one country or its citizens". The aim of conducting such activities is to incapacitate critical national infrastructure and in order to become more dependent on computer networks and therefore more vulnerable, creating a "massive electronic Achilles' heel" of each system that could be violated and misused by organized groups (Lewis, A. J., 2002). Cyber terrorism is actually using modern technology to exploit strategic weaknesses of a system and use those weaknesses for achieving its' goals.

Debra Littlejohn Shinder (2002:19) believes that attacks on computers and computer networks can be defined as cyber terrorism if the effects are destructive enough to produce fear comparable to the physical act of terrorism. This is a violent form of computer criminality committed, planned or coordinated in a virtual space and using computer networks. Some of the most common acts that lead to computer terrorism are: a) communication with electronic messages in order to carry out specific terrorist activities or to recruit new members for terrorist organizations; b) air traffic sabotage, in order to provoke crashing the aircrafts or water pollution by sabotaging electronic purifiers; c) incursions into hospital and healthcare systems, in order to delete or change patients' database and prescribed methods of treatment, or to attacks the power supply infrastructure, that can provoke the death of a large number of people who are on respirators etc.

Abraham R. Wagner (2005: 7) believes that the Internet and social networks are an ideal place to carry out terrorist activities and operations, because they allow geographically unlimited actions as well as high-speed

communications that do not cost much. The terrorists' use and misuse of computers and computer networks can be conducted in four main directions: (1) using Internet for terrorists communicating between each other; (2) creating access to a variety of information stored on the Internet and implying possible targets as well as providing technical details for such, (3) the use of the Internet to spread terrorist ideas and the ideology of a terrorist organization and (4) the conducting of terrorist attacks over the Internet.

An old Chinese dictum says that it is enough to kill one to scare thousands. Considering this, cyber terrorism is defined also as a criminal act in virtual space aim to intimidate the government of one country or its citizens for achieving some political objectives (Petrović, S., 2001:115). Technical characteristics of conducting such terrorist acts are unlimited opportunities for direct monitoring, control and disclosure of these activities; unlimited possibilities in time and space in virtual space, the possibility of operating at a large distance, numerous choices of targets, the lack of geographical constraints, precise timing, possibility for previous testing of planned actions which reduce the risk of eventual failure to a minimum; anonymity of the perpetrators. Internet terrorism is a deliberate misuse of digital information systems, networks or its' components in purpose of conducting terrorist activity and achieving its goal. The results of these activities are direct violence, spreading fear among civilians, causing instability of strategic and vital functions of the state institutions and great suffering of the civilians, as well as different mass accidents described as "collateral damage" (Dimovski, Z., Ilijevski, I., & Bebanoski, K., 2012:68).

Criminological dimensions of cyber terrorism

Terrorism, as a criminological phenomenon, is a necessary opponent to almost all modern societies, regardless of their level of socioeconomic development. Cyberterrorism can be considered as an "attractive option for modern terrorists, who value its anonymity, its potential to inflict massive damage, its psychological impact, and its media appeal" (Weinmann, G., 2005:130).

One of the international organizations that has devoted its work to combat cyber crime by setting up the National Infrastructure Protection Plan in 2013 is the American National Infrastructure Protection Center (NIPC). According to The Deputy Chief of Staff for Intelligence (DCSINT) Handbook No. 1.02 - Cyber Operations and Cyber Terrorism (2005: I-1) which is used for training US soldiers, internet terrorist operations consist of internet terrorism and internet support, expressed through planning, recruitment and propaganda. With this kind of activities, the computer network can be used as a weapon, as an intermediary target or as an activity that precedes or follows

physical assault. The Manual states that the most important goals of cyber terrorism is the loss of integrity of the target itself, reducing its possibilities of action, lack of trust, security and safety, and then finaly the physical destruction (DCSINT Handbook No. 1.02 - Cyber Operations and Cyber Terrorism, 2005: II-3). The most common motivation identified within cyber terrorism is blackmail, desire for destruction, different kinds of exploitation and revenge, and most common actions undertaken or threatened by terrorists are "physical destruction, destruction of important data and information, attack on computer systems of great importance, illegal incursions into computer systems from public importance and the access denial to essential systems, services and data" (DCSINT Handbook No. 1.02 - Cyber Operations and Cyber Terrorism, 2005: II-8). The FBI described cyber terrorism as a "development of terrorist capabilities provided by new technologies and networked organizations, which allows terrorists to conduct their operations with little or no physical risk to themselves" which is focused on "physical destruction of information hardware and software, or physical damage to personnel or equipment using information technology as the medium" (DCSINT Handbook No. 1.02 - Cyber Operations and Cyber Terrorism, 2005: II-2).

Based on the characteristics of cyber terrorism, according to Ashley, K. B. (2003), it is possible to reconstruct the criminological dimensions of the terrorist attacks in cyberspace. In order to understand better the cyber terrorism, it is necessary to first understand the virtual space itself with all its possibilities, and then to analyze the following questions:

(1) Who are the perpetrators of cyber terrorism (whether they are supported by a state, whether the state discards them, whether they are quasi-public formations, hacker groups or people in power who are engaged in espionage);

(2) What tools and techniques will be used in the process of planning and execution of the attack itself;

(3) How to apply the techniques, tactics and procedures for performing cyber attacks (a method of social engineering, creation and releasing of viruses and malware into the computer system);

(4) Where the attack is carried out or which categories of potential targets of terrorist cyber attacks (information and communication networks, data, objects in „real" world, energy, banking and finance, vital services of a country);

(5) Why the attack is carried out or the motivation for carrying out cyber terrorist attacks, which results they want to achieve, what are the advantages and disadvantages of such actions;

(6) When the attack is carried out.

Who are cyberterrorists and supporters of cyberterrorism and how do they communicate?

Cyber attackers have repeatedly demonstrated that they can jeopardize the functioning of an entire system of the state. The terrorists want to convey their message to a larger group of people; they need a global audience to spread their propaganda, to communicate and to recruit new members, and the Internet as a global communication medium allows them to do that. Threats and terrorist activity may vary according to the motivation of the holder of threat.

The former head of the FBI's cyber terrorism unit, Michael A. Vatis (2001) classified potential cyber attackers in four different categories:

- Terrorists, who use cyber attacks as a weapon;
- Terrorist sympathizers, who'll engage in terroristic activity because they share the same idea and belief as a certain terroristic group;
- Nations or states, who'll bet involved because they support certain terroristic goals or want to develop cyber warfare capabilities, and
- "Thrill seekers or cyber joyriders", who simply want to gain notoriety through high profile cyber attacks.

Some other authors, like Zoran Stojanovski *et al.* (Stojanovski, Z., Dojčinovski, M., & Ačkoski, J., 2012) state that as the perpetrators or contractors of acts of cyber terrorism may appear "different individuals, groups, organizations, national cells and even countries", which can be classified as:

- "Perpetrators beginners, whose skills and knowledge are not yet sufficiently developed and they most often use only hacker tools from the Internet;
- Perpetrators for fun, who possess greater knowledge and a wide range of hacking skills, they are motivated by curiosity and a desire for fun;
- Cyber activists, who know exactly which web sites they want to change and attack;
- Members of organized crime groups, who are highly motivated by profit, usually consist of well trained and skilled hackers who are working hard to develop this type of organized crime and making money, but usually have help and support from certain interest groups in society;
- Terrorist organizations or individuals who are sympathizers of terrorist organizations;
- State authorities that support certain professional hacker groups which execute precisely defined objectives and tasks;

- "Insiders", who are probably the most dangerous, because they have a lot of knowledge and skills, but they also have unlimited access to the network and the resources that are potential targets".

Terrorists in cyberspace can often use different steganographic tools and encryption methods. Steganography represents the scientific discipline that studies the methods of hiding secret messages within the media of harmless character and the covert exchange of information (Spasić, V., & Vasić, A., 2012). It represents the "hidden writing" ie. the process of hiding secret messages inside some multimedia files (like photo, audio or video file), which usually contain unused or irrelevant data spaces filled by terrorists' secret information, using different steganographic techniques. The perpetrator can input hidden message in a digitized visual and audio data, which not bother the original multimedia message, but can only be discovered if searched for in a specific way. The steganography process generally involves inserting secret messages inside a transmission medium, which is called a "carrier", and which has the role of concealing secret messages. The unity consists of the secret message and the "carrier" in which the message was incorporated, which is called steganography media or stego.

Encryption is a way to protect certain content against unwanted and unauthorized reading or change of data. The protection level is determined by an algorithm or key ("encryption algorithm"). There are two types of encryption systems ("cryptosystems"): symmetric and asymmetric. A symmetric system of encryption uses the same "secret key" which is used both for encryption and decryption, and the asymmetric system of encryption uses one public key to encrypt messages, and other, secret one, for decryption. There is a perception that members of Al Qaeda communicate by sending encrypted messages like this. Today, the encryption is not so widespread as before, because intelligence services have developed strong systems for decoding the encryption. Encryption and encrypted messages are still present on various internet forums, where terrorist organizations often leave their messages in the form of encrypted text messages to terrorist cells, which they can then publicly read. Identification of users that use this kind of encrypted communication for terrorist purposes on some internet forums is almost impossible.

Nowadays, members of terrorist organizations and task forces mostly conduct their operations in the cyberspace via e-mail, which is checked through a free and anonymous webmail account (like Yahoo, Gmail, etc.). Intelligence services have the technology only to monitor the correspondence between the particular electronic addresses and e-mails sent from these accounts. However, if the message has not been sent from specified e-mail addresses to some different user account or to some other network, the intelligence agencies now have no way to monitor what happens to those open

virtual mailboxes. User name and password of the certain webmail account is given to members of certain operative terroristic groups in order not to communicate by sending e-messages to other addresses, but to exchange messages with each other by leaving the messages in a folder labeled "drafts". This way, all the members who have a username and password of the same e-mail, checked over the network using that address and the "draft" folder cannot read the message that they left behind, which is most likely to represent a set of operational instructions or actions of the terrorist group. The probability that someone other than members of the terrorist organization will read these messages are very small, because the message is not sent but remains stored in the virtual space in a particular user account through which the communication takes place.

Why do the terrorists rely on cyberspace and social networks?

The most common and obvious reasons why the terrorists rely on cyberspace are because it is significantly cheaper, completely anonymous, the variety and number of targets and potential victims are enormous and just "a click away" – there is no need to cross any distance or to be seen as a perpetrator. By using the Internet, because of its availability and distribution, it is easier to recruit and mobilize new supporters of terrorist ideas, to find information and facilities regardless of the part of the globe where they are physically located, it is easier to find sources of financing, to build connections for the implementation of joint actions, to exchange information and to educate new members for illegal activities. It is important to be aware of the effects of psychological warfare, because this way fear and panic can spread faster by the methods of disinformation, threats and setting the terrifying images of torture and executions.

Various sensitive state and social structures can be attacked and affected with different methods of attack, in addition different weapons can be used. Most of the terrorist groups use three basic methods: physical attack carried out with conventional weapons and directed to computer systems or data information transmission lines; electronic attack that involves the use of electromagnetical force or electromagnetic pulse to block computer systems, the insertion of malicious software into the computer systems and channels of information transfer, as well as the attack on the computer networks that usually involves the use of malware as a function of weapons in computer and network systems and exploitation of the vulnerabilities and weaknesses in computer programs, used by the enemy in system configuration or security settings of your computer in order to steal some data or destroy them (Rodriguez, C. A., 2006). Terrorist organizations largely take advantage of the Internet in order to carry out their activities: in 1998 more than half of the organizations that had been identified in the United States as terrorist had a

website, in 1999 all had at least one internet presentation, and by 2007 it is recorded that there were over 5,000 terrorist websites on the internet. Basically all terrorist web sites contain information such as basic goals and mission, the history of the organization, the arguments which appeals to potential new members to accept the mission and goals of the organization, audio and video attachments, recognizable logos of organizations and even video games for children ideologically promoting the goals of terrorist organizations (Kešetović, Ž., & Blagojević, M., 2012).

According to Weimann (2004), there are many reasons why terrorists use the internet for propaganda, planning and implementation of its activities, as well as the recruitment of new members: (1) the internet is cheap because all you need is "a personal computer and an online connection", it is not necessary to purchase arms because only one malicious program is enough to realize certain activity; (2) the manner of conducting the attack "protects the anonymity of the attackers who use different nicknames so it is difficult to trace them, there are no geographical borders between different countries nor police checkouts to deal with"; (3) the number of potential targets is impossible to determine; (4) for the implementation of planned terroristic actions it takes less physical training and readiness, the risk of death is insignifficant and it is not necessary to travel to different places and (5) cyber terrorism can affect many more people than traditional terrorist attacks (Weimann, G., 2004: 6).

In addition to conventional weapons, terrorists can now also use modern, strong and massive weapons such as the mass media and new technologies. For instance, the internet network can be used in one of the triple ways: "as a weapon, as a medium and as a goal for itself" (Gaćinović, R., 2012:16). It is important as a communication tool between activists and for addressing the public in order to spread terroristic ideology. The fastest way to spread fear and panic is "through mass media and technology in general" (Babić, V., 2015:12). Using encrypted communications through the public Internet service provides "an opportunity for members of the various terroristic cells to be in constant contact, making their detection and the interpretation of sent messages very difficult" (Ranđelović, D., Bajagić, M., & Carević, B., 2012: 318). In addition to communication via e-mail, there are other techniques for communication and data exchange via Internet, such as embedding data into digital images and "dead drop" technique (Ranđelović, D., Bajagić, M., & Carević, B., 2012: 322). The sender can incorporate certain information into digital images available on the Internet or can replace an existing image with one that already contains data, so the recipient can download images from the Internet and to extract the data, with no apparent link to the sender (embedding data into digital images) or use certain place on the server as a file sender while the recipient of the files can be removed or

hidden; any available server can be used, the name of the file remains on the server, but not its' content (so called "dead drop"). There are numerous public and private services on the Internet that could be potential targets of terrorist attacks, such as information and communication systems, banking and finance, energy (oil, gas, electricity), delivery of commercial products and services considered vital for human beings (Ranđelović, D., Bajagić, M., & Carević, B., 2012: 324).

Social networks can be used by terrorists for the purpose of psychological weapons in order to spread disinformation spreading fear, panic, intimidating messages and threats to the public (Babić, V., 2015:13). Terrorists have a complete control over the contents of messages that are placed in the electronic media and on social networks, and that is just one more way of trying to collect funds to finance its activities, for the recruitment and mobilization of new members[3] for the purpose of building connections and exchange of information, planning and coordination of terrorist activities.[4]

Funding a terrorist organization can also be done over the Internet and through social networks. Numerous terrorist groups seek direct financial contributions from its site visitors and from its members and supporters: the money can be paid directly to specific bank accounts, and some organizations are receiving donations and using PayPal service or sales in online stores which are located within their web presentations (Kešetović, Ž., & Blagojević, M., 2012:48). Donations are not necessarily in cash, but may also be in the actions and objects that terrorist activitists may find to be of help for the main activity (weapons, maps for buildings and objects of interest, bulletproof vests, etc.). In order to gain funds for financing terrorist activities, members of terrorist groups are also very often keen to commit other criminal acts, such as the abuse or misuse of different tools for e-commerce, debit or credit cards, theft of someone else's identity, internet scams etc.

[3]Internet could be the initial contact point for individuals who voluntarily want to join terrorist movements, because they used the Internet to spread their propaganda and ideology by uploading different literature for the purpose of recruiting potential members, identification of possible interests and for presentation of different ideas based the distorted interpretation of religious beliefs etc. *See:* Babić, Vladica, 2015:18

[4]Terrorists use the Internet in order to plan and to coordinate specific attacks, in which they use encrypted messages via chat rooms, maps, photographs, signs, technical features hidden in graphics files and digital images, as well as different steganographic tools. *See:* Babić, Vladica, 2015: 22

How to fight cyber terrorism at the international level?

The Annual Report of the United Nations Office on Drugs and Crime (UNODC) stated that the lack of an international agreement on cybercrime and terrorism is thwarting efforts to bring terrorists to justice, and concluded that nations should consider a universal agreement that require the countries to cooperate with each other during cybercrime and cyber terrorism investigations (Gross, G., 2012). The Report (UNODC Annual Report, 2015) appealed to the national legislations that they need to established practices for fighting cyber terrorists and for the successful prosecution of such cases, by implementing several recommendations:

(1) Law enforcement agencies should work together with Internet service providers to collect "key evidence" in cyber terrorism cases;

(2) Operators of Wi-Fi networks and cybercafés should consider requiring from their users to register and to identify themselves;

(3) National governments should outlaw terrorist activity online and by regulating ISP addresses, because the terrorists have access to the public Internet, including airport and library Wi-Fi hotspots; as well as to maintain human rights protections.

UNODC, in collaboration with the United Nations Counter-Terrorism Implementation Task Force (CTITF), developed and published in October 2012, a new technical assistance tool named The Use of the Internet for Terrorist Purposes (2012), This technical assistance tool aims to provide practical guidance for policy makers, investigators and prosecutors on effective criminal justice responses to cases involving the use of the Internet for terrorist purposes (Countering the Use of the Internet for Terrorist Purposes, 2012). The publication explained number of cases where the cyberspace is used "as a tool for the glorification of terrorist acts, incitement, recruitment and radicalization, financing, training, planning and the commission of terrorist attacks, and provides an overview of the applicable legal good practices identified in the conduct of investigations, evidence gathering and prosecution of such cases, while exploring potential opportunities to strengthen inter-State and private sector cooperation in this regard" (*Ibid.)*. However, the publication does not cover all uses of the Internet for terrorist purposes and the issues of cyber-crime, like cyber attacks and the preservation of cyber security.

International legislation made great efforts to effectively counter fight cyber terrorism, both on international as well as at member states level, emphasizing the interstate and intergovernmental cooperation on three parallel levels:

(1) Through international organizations: the United Nations requires of its Member States to put special measures to prevent all potential hazards in the field of information security, while in September 2002 Interpol established a special department against terrorism (Interpol – Counter-Terrorism Fusion Centre);

(2) Through multilateral and multinational platforms: the interest of the G8 dealing with the prevention of terrorism and protection of information technology from terrorism, and through the work of the Organization for Economic Cooperation and Development (OECD) which in 2002 adopted Guidelines for the Security of Information Systems and Networks by suggesting the governments of member states to promote information security and the security of computer networks in order to prevent cyber terrorism, computer viruses and hacking into systems, so that the privacy of individuals and their personal freedom would be safe;

(3) Through regional action: mostly through the activities of the European Union against terrorism in general and the Council of Europe, by establishing The Committee of Experts on Cyber Terrorism (CODEXTER)[5] and the adoption of the Convention on Cybercrime CETS No. 185 (2001) and the Convention on the Prevention of Terrorism CETS No. 196 (2005).

In past few years, the scientists have been trying to find the way how to fight against terroristic activities on "Dark Web" and in cyberspace. Using advanced techniques, such as Web networking, link analysis, content analysis, authorship analysis, sentiment analysis and multimedia analysis, experts can find, catalogue and analyze extremist activities online, using the power of advanced computers and applications to find patterns and connections where

[5]CODEXTER at its meetings concluded that the Internet can be used for terrorist purposes in several different ways and can its use can produce different effects: 1) terrorist attacks over the Internet can cause harm not only to the electronic communication systems but also to "ordinary" infrastructure systems and to produce a large number of human casualties; 2) dissemination and distribution of illegal content, threats, advertisements that glorify terrorism, financing of terrorist acts, organizing training for terrorist and potential member recruitment for terrorist organizations, and 3) the use of logistics and information technology in order to research for potential targets of terrorist attacks. *See:* Council of Europe – Action against Terrorism, RetrievedDecember 07, 2016 from http://www.coe.int/t/dlapil/codexter/default_EN.asp, retrieved 07. 12. 2016. and Council Of Europe - Opinion Of The Committee Of Experts On Terrorism (Codexter) For The Attention Of The Committee Of Ministers On Cyber terrorism And Use Of Internet For Terrorist Purposes, http://www.coe.int/t/e/legal_affairs/legal_cooperation/fight_against_terrorism/4_theme_files/Cyberterrorism.asp#TopOfPage, retrieved 07. 12. 2016.

humans can not. "Writeprint" technique is one of the tools developed by Dark Web, which automatically extracts thousands of multilingual, structural, and semantic features to determine who is creating 'anonymous' content online, and the experts also use complex tracking software called "Web spiders" to search discussion threads and other content to find Internet discussions where terrorist activities are taking place (*Scientists Use the 'Dark Web' to Snag Extremists and Terrorists Online,* n.d.).

Conclusion

In the era of information technology, terrorism can be seen as conventional terrorism, in which classical weapons (explosives, guns, etc.) are used for the destruction of resources and personnel in a physical sense; techno terrorism, in which the classic ordnance are used for destroying infrastructure and causing damage in cyberspace; and as cyber terrorism, where new weapons (malicious software, electromagnetic and microwave weapons) are used for the destruction and modification of data in cyberspace.

Because of the cyber terrorism phenomenon and its frequency, security agencies responsible for investigating terrorism, including cyber terrorism, must remain vigilant, which includes ensuring adequate funding for staffing, equipment, and training, encouraging citizens to be alert and to report any suspicious behavior (Tafoya, W. L., 2011). The possibility that the next generation of terrorists, who are now growing up in a digital world, where hacking tools are sure to become more powerful, more simple to use and much easier to access (Weinmann, G., 2005), would be able to see predict much more danger in future cyber terrorist acts is terrifying.

Precautions are necessary in order to protect people from the physical threats, and that is the reason why security agencies should be prepared to deal with cyber attacks on the nation's critical infrastructure which are hard-to-forecast and very often reoccurring.

Constant efforts to educate professionals and Internet users, raising the culture of safety in the cyberspace, cleverly designed and continuously adaptive technological, organizational and regulatory measures may have an impact on the prevention of cyber terrorism, to reduce risks to an acceptable level, and ultimately, to keep the scale of civilization progress in the cyberspace, not its destruction. Potential future conflicts will involve new participants in the global geopolitical level, but also an independent hackers, hackers sponsored by the state itself, cyber criminals and cyber terrorists. Battlefields are not anymore physically located in certain country and geographically specific, but warfare and conflict has reversed in the virtual environment and in global networks, where the concept of time was changed because the attack is immediate and unpredictable. In cyber attack the element of surprise is vital, and its dynamics is variable from day to day. For this

reason, the key question is whether and how the cyberspace can be fully controlled, how to adopt appropriate legal framework due to the dynamic of cyber development and the treatment procedures which are rather slow, and how to find out who are the perpetrators, were they come from and how to prosecute and sanction them.

References

Anonimus. (2015). *The Deep Web – Mračna strana Interneta (The Deep Web – Dark side of the Internet).* Beograd: Laguna.

Ashley, K. B. (2003). *Anatomy of cyber terrorism: Is America vulnerable?* USA: Air University, Maxwell AFB, AL.

Babić, V. (2015). Novi oblici djelovanja terorista (Cyber terorizam). 4th International Scientific and Professional Conference 'Police College Research Days In Zagreb', 23-24 April, 2015. 11-26. Retrieves December 15, 2016 from http://www.mup.hr/UserDocsImages/PA/vps/idvps2015/Zbornik_radova_Konferencije.pdf

Collin, C. B. (n.d.). The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge. 11th Annual International Symposium on Criminal Justice Issues. Retrieved February 02, 2017 from http://www.crime-research.org/library/Cyberter.htm

Council of Europe – Action against Terrorism. *(n.d.).* Retrieved December 07, 2016 from http://www.coe.int/t/dlapil/codexter/default_EN.asp

Council of Europe - Convention on Cybercrime CETS No. 185. (2001)

Council of Europe - Convention on the Prevention of Terrorism CETS No. 196. (2005).

Council Of Europe - Opinion Of The Committee Of Experts On Terrorism (Codexter) For The Attention Of The Committee Of Ministers On Cyber terrorism And Use Of Internet For Terrorist Purposes. *(n.d.).* Retrieved December 07, 2016 from http://www.coe.int/t/e/legal_affairs/legal_cooperation/fight_against_terrorism/4_theme_files/Cyberterrorism.asp#TopOfPage

Countering the Use of the Internet for Terrorist Purposes, 2012, UN Office on Drugs and Crime. Retrieved February 05, 2017 from https://www.unodc.org/unodc/en/terrorism/news-and-events/use-of-the-internet.html

DCSINT Handbook No. 1.02, Cyber Operations and Cyber Terrorism. (2005). Retrieved December 24, 2016 from http://www.globalsecurity.org/military/library/policy/army/other/tradoc-dcsint-hbk_1-02-2005.pdf

Dimovski, Z., Ilijevski, I., & Bebanoski, K. (2012). Bezbedonosno-kriminalističke dimenzije sajber-terorističkih napada. *Zbornik radova, Međunarodna naučnostručna konferencija, Suzbijanje kriminala i evropske integracije s osvrtom na visokotehnološki kriminal, Laktaši 28 - 30. 03. 2012.*, 65-78

Gaćinović, R. (2012). *Oblici savremenog terorizma*. Nauka, bezbednost, policija, Institut za političke studije, Beograd, 17(1), 1-17

Gross, G. (2012). UN: More international cooperation needed to fight cyberterrorism. Computernews World from October 24, 2012. Retrieved February 02, 2017 from http://www.computerworld.com/article/2492864/cybercrime-hacking/un--more-international-cooperation-needed-to-fight-cyberterrorism.html

Hack Defence. *(n.d.)* Retrieved December 2, 2017 from http://hackdefencesecurity.blogspot.rs/2012/02/1.html

Interpol - Counter-Terrorism Fusion Centre. (n.d.). Retrieved December 12, 2016 from http://www.interpol.int/Crime-areas/Terrorism/Counter-Terrorism-Fusion-Centre

Kešetović, Ž., & Blagojević, M. (2012). Internet i terorizam. *Zbornik radova, Međunarodna naučnostručna konferencija, Suzbijanje kriminala i evropske integracije s osvrtom na visokotehnološki kriminal, Laktaši 28 - 30. 03. 2012.*, 43 – 52

Lewis, A. J. (2002). Assessing the Risks of Cyber Washington DC, Terrorism, Cyber War and Other Cyber Threats". *Center for Strategic and International Studies*. Retrieved january 17, 2017 from http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

Littlejohn Shinder, D. (2002). *Scene of the Cybercrime: Computer Forensics Handbook*. USA; Rockland, MA: Syngress Publishing Inc.

Manap., N.A., & Tehrani, P.M. (2012). Cyber Terrorism: Issues in Its Interpretation and Enforcement. *International Journal of Information and Electronics Engineering*, 2(3), 409-413

National Infrastructure Protection Plan. (2013). Retrieved January 16, 2017 from http://www.dhs.gov/national-infrastructure-protection-plan

OECD Guidelines for the Security of Information Systems and Networks: towards a culture of security. (2002). Retrieved January 02, 2017 from http://www.oecd.org/sti/ieconomy/15582260.pdf

Petrović, S. (2001). Kompjuterski kriminal. Beograd: MUP Republike Srbije

Ranđelović, D., Bajagić, M., & Carević, B. (2012). Internet u funkciji terorizma. *Zbornik radova, Međunarodna naučnostručna konferencija, Suzbijanje kriminala i evropske integracije s osvrtom na visokotehnološki kriminal, Laktaši 28 - 30. 03. 2012.*, 317-330

Rodriguez, C. A. (2006). *Cyber terrorism – A rising threath in the Western hemisphere*. USA: Fort Lesley J. McNair, Washington DC

Scientists Use the 'Dark Web' to Snag Extremists and Terrorists Online. (n.d.). Retrieved February 05, 2017 from http://phys.org/news/2007-09-scientists-dark-web-snag-extremists.html

Spasić, V., & Vasić, A. (2012). Steganografija u funkciji zaštite podataka na Internetu. *Zbornik Pravne infrastrukturne osnove za razvoj ekonomije zasnovane na znanju, Kragujevac: Pravni fakultet, 2012*, 257-274

Stewart, S. (2015, Octobar). The Coming Age of Cyberterrorism. *Security Weekly from October 22, 2015*. Retrieved January 27, 2017 from https://www.stratfor.com/weekly/coming-age-cyberterrorism

Stojanovski, Z., Dojčinovski, M., & Ačkoski, J. (2012). *Sajber terorizmot – Zakana za komunikacisko-informaciskite sistemi.* Skopje: Voena akademija "General Mihailo Apostolski". Retrieved January 30, 2017 from http://eprints.ugd.edu.mk/6537/1/__ugd.edu.mk_private_UserFiles_biljana.kosturanova_Desktop_Trudovi_Jugoslav%20Achkoski_Scientific%20Papers_elektronska%20verzija_Sajber%20terorizmot%20-%20zakana%20za%20komunikacisko-informaciskite%20sistemi%20-%20Zoran%20Stojanovski.doc

Tafoya, W. L. (2011). Cyber Terror. *FBI Law Inforcement Bulletin*, November 2011, 80 (11)

Techopedia. *(n.d.).* Retrieved December 2, 2017 from http://www.interpol.int/Crime-areas/Terrorism/Counter-Terrorism-Fusion-Centre

The Use of the Internet for Terrorist Purposes. (2012). Retrieved February 02, 2017 from https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

UNODC Annual Report. (2015). Retrieved February 02, 2017 from http://www.unodc.org/documents/AnnualReport2015/Annual_Report_2016_WEB.pdf

Vatis, M. A. (2001). Cyber Attacks During the War on Terrorism: A Predictive Analysis. *Special Report, Institute for Security and Technology Studies.* Retrieved February 03, 2017 from http://www.ists.dartmouth.edu/docs/cyber_a1.pdf

Wagner, R. Abraham (edt., 2005). Fighting Terror in Cyberspace, Terrorism and the internet: use and abuse. Retrieved January 17, 2017 from https://books.google.rs/books?id=yf83KZZbeQIC&pg=PA1&lpg=PA1&dq=Wagner,+A.,+R.:+%22Fighting+Terror+in+Cyberspace,+Terrorism+and+the+internet:+use+and+abuse&source=bl&ots=OcEV_qWD_5&sig=o4qzKdNYafWWEKAby_yuksVhApM&hl=sr&sa=X&ved=0ah

UKEwj3yIvsoOrJAhVC1RoKHSU6DMQQ6AEIITAB#v=onepage&q=Wagner%2C%20A.%2C%20R.%3A%20%22Fighting%20Terror%20in%20Cyberspace%2C%20Terrorism%20and%20the%20internet%3A%20use%20and%20abuse&f=false

Weimann, G. (2004). Cyber terrorism - How Real Is the Threat? *Special report 119, United States Institute of Peace, Washington, DC*. Retrieved January 17, 2017 from http://www.usip.org/files/resources/sr119.pdf

Weinmann, G. (2005). Cyberterrorism: The Sum of All Fears? *Studies in Conflict & Terrorism,* 28, 129–149, DOI: 10.1080/10576100590905110

Wilson, C. (2005). Computer Attack and Cyber terrorism: Vulnerabilities and Policy Issues for Congress. *CRS Report for Congress*. Retrieved January 17, 2017 from https://fas.org/irp/crs/RL32114.pdf