# CYBER TERRORISM ON THE INTERNET AND SOCIAL NETWORKING: A THREAT TO GLOBAL SECURITY

Vida M. Vilić

Clinic of Dentistry Niš

Abstract:

In recent years, an increasing problem attracting expert attention has been the “dark side of surfing the Internet” or “Dark net” or “Deep Web”. It is estimated that this “digital underground” is much bigger than the Internet itself and that hackers, criminals, terrorists, paedophiles can completely freely carry out their illegal activities. Cyber space is very suitable for various terrorist activities and operations, as it provides a facility for secure communications at a very low cost, while social networks can be used by terrorists as a psychological weapon.

Cyber terrorism is a modern form of terrorism, which connects two great fears of modern times: the virtual space and terrorist activity. Most of the terrorist groups use three basic methods: physical attack, electronic attack and the attack on the computer networks. Based on the characteristics of cyber terrorism, it is possible to reconstruct the criminological dimensions of terrorist attacks in cyberspace.

International legislative made great efforts in order to effectively counter fight cyber terrorism both on international as well as on member states level, emphasizing the interstate and intergovernmental cooperation on three parallel levels:  international organizations, multilateral and multinational platforms and regional action.

Keywords:

cyber space, cyber terrorism, characteristics of cyber terrorism, methods, social networks, international legislative.

## 1. INTRODUCTION

In recent years, an increasing problem attracting expert attention has been the “dark side of surfing the Internet” or “Dark net” or “Deep Web”, where data and information is password locked, trapped behind a pay walls, or the user is required to use special software to access this data. It is estimated that this “digital underground” is much bigger than the Internet itself and that hackers, criminals, terrorists, paedophiles can completely freely carry out their illegal activities. In Deep Web users can buy and sell drugs, forged money and forged documents, weapons, ammunition and explosives, order and pay to murder someone, sell and buy human organs. Deep Web has a special system of online payments concealing identity [1]. Considering that those activities on Deep Web and especially cyber terrorism are a new area of possible computers and networks misuse and

Correspondence:
Vida M. Vilić

e-mail:
vila979@gmail.com

DOI: 10.15308/Sinteza-2017-68-73

criminality, there is an evident lack of comprehensive theoretical and empirical research on this phenomenon.

## 2. WHAT IS CYBER TERRORISM

Cyber terrorism is a modern form of terrorism, which connects two great fears of modern times: the virtual cyber space and terrorist activity [2]. Internet space is very suitable for various terrorist activities and operations, as it provides a facility for secure communications at a very low cost [3]. Cyber terrorism refers to deliberate, politically motivated attacks on computer systems and programs, as well as the data, which could provoke violence and fear with the civilian targets [4]. New weapons in virtual wars that are used are Logic Bombs, Trojan horses, Worms and Viruses, whose main objective is to disable the system from functioning properly and the loss of information, so therefore to overload phone lines, air force control and to control computers responsible for supervision of other forms of transport, to lead to misuse and failure of programs used by large institutions of state significance and emergency services.

There is no unique and universally accepted definition of cyber terrorism, but all given definitions pointed 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 etc. However, internet terrorism must be considered separately from computer crime in general, because every attack on computer or network system does 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. For this reason, cyber terrorism is proper to define as the use of computers in the function of weapons or targets, by politically motivated international or para-national groups or individuals who threaten or carry out violence in order to influence the public and the official government to change their way of doing politics [5]. Some authors, such as James Lewis, 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, etc.) or to intimidate or compel a government of one country or its citizens [6]. 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, create a “massive electronic Achilles’ heel” of each system that could be violated and misused by organized groups [7]. Cyber terrorism is actually using modern technology to create strategic weaknesses of a system and use those weaknesses for achieving its goals.

Debra Littlejohn Shinder 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 [8]. This is a violent form of computer criminality committed, planned or coordinated in a virtual space and using computer networks [9]. Some of the most common acts that lead to computer terrorism are: communication with electronic messages in order to achieve agreed conspiracy to carry out specific terrorist activities or to recruit new members for terrorist organizations, air traffic sabotage in order to provoke crashing the aircrafts, water pollution by sabotaging electronic purifiers, incursions into hospital and healthcare systems to delete or change patients’ database and prescribed methods of treatment, attacks on infrastructure of power supply that can provoke the death of a large number of people who are on respirators, who are given medical care in their homes and do not have electrical generators as hospitals do etc.

Abraham R. Wagner 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 the computers and computer networks can be conducted in four main directions: (1) using Internet for terrorists communicating among 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, as for example concluding and handling the weapons; (3) the use of the Internet to spread terrorist ideas and the ideology of a terroristic organization and (4) the conducting of terroristic attacks over the Internet [10].

Cyber terrorism is defined also as a criminal act in virtual space aimed to intimidate the government of one country or its citizens for achieving some political objectives [11]. Technical characteristics of conducting such terrorist acts are limited 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 for the 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" [12].

## 3. CRIMINOLOGICAL DIMENSIONS OF CYBER TERRORISM

One of the international organizations that devoted its work to cyber crime is the American National Infrastructure Protection Centre - NIPC [13]. According to „DCSINT Handbook No. 1.02, Cyber Operations and Cyber Terrorism" which is used for training US soldiers, internet operations consist of internet terrorism and internet support, expressed through planning, recruitment and propaganda [14]. 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 goal 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 finally the physical destruction [15]. 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 [16]. 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"[17].

Based on the characteristics of cyber terrorism, 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 firstly to 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 [18].

## 4. WHY DO TERRORISTS RELY ON CYBER SPACE AND SOCIAL NETWORKS

Various sensitive state and social structures can be attacked and affected by different methods of attack, and also 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 electromagnetic force or electromagnetic pulse to block computer systems, as well as 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 [19]. Terrorist organizations largely take advantage of the Internet in order to carry out their activities: in 1998 more than half of the organizations that have been identified in the United States as terrorist had its website, in 1999 all had at least one internet presentation, and by 2007 it was 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 appeal 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. [20].

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 computer and access to the network, 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 insignificant and it is not necessary to travel to different places and (5) cyber terrorism can affect far more people than traditional terrorist attacks [21].

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 can be used in one of the triple ways: as a weapon, as a means of communication between activists and as a medium for addressing the public in order to spread terroristic ideology [22]. The fastest way to spread fear and panic is through mass and electronic media [23]. Using encrypted communications through the public Internet service provides provide 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 [24]. In addition to communication via e-mail, there are other techniques [25] for communication and data exchange via Internet, such as embedding data into digital images [26] and "dead drop" technique [27]. 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 extract the data, with no apparent link to the sender. Certain place on the server can be used as file sender, and the recipient of the files can be removed or hidden. For this purpose any available server can be used, the name of the file remains on the server, but not its content. 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 and electricity), delivery of commercial products and services considered vital for human beings [28].

Social networks can be used by terrorists as a psychological weapon in order to spread disinformation spreading fear, panic, intimidating messages and threats to the public [29]. 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 [30], for the recruitment and mobilization of new members [31], for the purpose of building connections and exchanging information [32], planning and coordination of terrorist activities [33]. By monitoring internet web sites, terrorist organizations can identify things that internet users are interested in and, accordingly, to make requests for payment of grants or donations for financing their actions. 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 on distorted interpretation of religious beliefs etc. 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.

Funding terrorist activities can also be done over the Internet and through social networks. Numerous terrorist groups seek direct financial contributions from its sites 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 [34]. 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 of 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 different 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.

## 5. CONCLUSION

International legislative made great efforts in order to effectively counter fight cyber terrorism both on international as well as on 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 [35];
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 [36] 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) [37] and the adoption of the Convention on Cybercrime [38] and the Convention on Prevention of Terrorism [39]. CODEXTER concluded at its meetings 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 search for potential targets of terrorist attacks.

## REFERENCES

[1] Anonimus: Deep Web – Mračna strana interneta, Laguna, Beograd, 2015.

[2] Abdul Manap Nazura, Moslemzadeh Tehrani Pardis, "Cyber Terrorism: Issues in Its Interpretation and Enforcement", International Journal of Information and Electronics Engineering, Vol. 2, No. 3, May 2012, pp. 409, http://www.ijiee.org/papers/126-I149.pdf, retrieved 16. 01. 2017.

[3] Ranđelović, Dragan, Bajagić, Mladen, Carević, Bojana, "Internet u funkciji terorizma", Zbornik radova, Međunarodna naučnostručna konferencija, Suzbijanje kriminala i evropske integracije s osvrtom na visokotehnološki kriminal, Laktaši 28-30.03.2012., pp. 318

[4] Gaćinović, Radoslav, „Oblici savremenog terorizma", NBP Žurnal za kriminalistiku i pravo, Kriminalističko-policijska akademija, 2012, pp. 15, http://www.kpa.edu.rs/cms/data/akademija/nbp/NBP_2012_1.pdf, retrieved 17. 01. 2017.

[5] Wilson, Clay, "Computer Attack and Cyber terrorism: Vulnerabilities and Policy Issues for Congress", CRS Report for Congress, 2005, pp. 5 and pp. 7, https://fas.org/irp/crs/RL32114.pdf, retrieved 17. 01. 2017.

[6] Lewis, A., James, "Assessing the Risks of Cyber Washington DC, Terrorism, Cyber War and Other Cyber Threats", Center for Strategic and International Studies, 2002, pp.1, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf, retrieved 17. 01. 2017.

[7] *Ibid.*

[8] Littlejohn Shinder, Debra: "Scene of the Cybercrime: Computer Forensics Handbook", Computer Forensics Handbook", 2002, p. 19, http://www.dvara.net/hk/Syngress%20Scene%20of%20the%20CyberCrime.pdf, retrieved 24. 12. 2016.

[9] *Ibid.*

[10] Wagner, R. Abraham, "Fighting Terror in Cyberspace, Terrorism and the internet: use and abuse", Series in Machine Perception and Artificial Intelligence – vol.6, 2005, pp. 7

[11] Petrović, Slobodan: Kompjuterski kriminal, MUP Republike Srbije , 2001, pp. 115

[12] Dimovski, Zlate, Ilijevski, Ice, Bebanoski, Kire, "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., pp. 68

[13] National Infrastructure Protection Plan, http://www.dhs.gov/national-infrastructure-protection-plan, retrieved 16. 01. 2017.

[14] DCSINT Handbook No. 1.02, Cyber Operations and Cyber Terrorism, 2005, pp. I-1, http://www.globalsecurity.org/military/library/policy/army/other/tradoc-dcsint-hbk_1-02-2005.pdf , retrieved 24. 12. 2016.

[15] DCSINT Handbook No. 1.02, Cyber Operations and Cyber Terrorism, *op.cit.*, 2005, pp. II-3

[16] DCSINT Handbook No. 1.02, Cyber Operations and Cyber Terrorism, *op.cit.*, 2005, pp. II-8

[17] DCSINT Handbook No. 1.02, Cyber Operations and Cyber Terrorism, *op.cit.*, 2005, pp. II-2

[18] Ashley, K. Bradley, "Anatomy of cyber terrorism: Is America vulnerable?", Air University, Maxwell AFB, AL, 2003, www.au.af.mil/au/awc/awcgate/awc/ashley.pdf, retrieved 17. 01. 2017.

[19] Rodriguez, A., Carlos, "Cyber terrorism – A rising threath in the Western hemisphere", Fort Lesley J. McNair, Washington DC, 2006, http://www.library.jid.org/en/mono45/Rodriguez,%20Carlos.pdf, retrieved 17. 11. 2016.

[20] *See*: Kešetović, Želimir, Blagojević, Marija, "Internet i terorizam", Zbornik radova, Međunarodna naučnostručna konferencija, Suzbijanje kriminala i evropske integracije s osvrtom na visokotehnološki kriminal, Laktaši 28-30.03.2012., pp. 47

[21] Weimann, Gabriel, Cyber terrorism - How Real Is the Threat?", Special report 119, United States Institute of Peace, Washington, DC, 2004, http://www.usip.org/files/resources/sr119.pdf, retrieved 17. 01. 2017.

[22] Gaćinović, Radoslav, *op.cit.*, 2012, pp. 16

[23] Babić, Vladica, „Novi oblici djelovanja terorista (Cyber terorizam)", 4th International Scientific and Professional Conference 'Police College Research Days In Zagreb', pp. 12

[24] Ранђеловић, Драган, Бајагић, Младен, Царевић, Бојана, *op.cit.*, 2012, pp. 318

[25] *See*: Ранђеловић, Драган, Бајагић, Младен, Царевић, Бојана, *op.cit.*, 2012, pp. 322

[26] *See*: Ранђеловић, Драган, Бајагић, Младен, Царевић, Бојана, *op.cit.*, 2012, pp. 322

[27] *See*: Ранђеловић, Драган, Бајагић, Младен, Царевић, Бојана, *op.cit.*, 2012, pp. 322

[28] Ранђеловић, Драган, Бајагић, Младен, Царевић, Бојана, *op.cit.*, 2012, pp. 324

[29] Бабић, Владица, *op.cit.*, 2015, pp. 13

[30] *See*: Бабић, Владица, *op.cit.*, 2015, pp. 17

[31] *See*: Бабић, Владица, *op.cit.*, 2015, pp. 18

[32] Бабић, Владица, *op.cit.*, 2015, pp. 20

[33] *See*: Бабић, Владица, *op.cit.*, 2015, pp. 22

[34] Кешетовић, Желимир, Благојевић, Марија, *op.cit.*, 2012, pp. 48

[35] *See*: Interpol - Counter-Terrorism Fusion Centre, http://www.interpol.int/Crime-areas/Terrorism/Counter-Terrorism-Fusion-Centre, retrieved 12. 12. 2016.

[36] OECD Guidelines for the Security of Information Systems and Networks: towards a culture of security, http://www.oecd.org/sti/ieconomy/15582260.pdf, retrieved 02. 01. 2017.

[37] *See*: Council of Europe – Action against Terrorism, http://www.coe.int/t/dlapil/codexter/default_EN.asp, retrieved 07. 12. 2016.

[38] Convention on Cybercrime CETS No. 185, 2001, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, retrieved 07. 01. 2017.

[39] Convention on the Prevention of Terrorism CETS No. 196, 2005, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008371c, retrieved 16. 12. 2016.