Terrorist activities and internet government with focus on importance of prevention within a family

Zaklina Spalevic[1], Milan Pocuca[2], Zeljko Bjelajac[2]

[1] Faculty of Law, University Sinergija, Bijeljina, Bosnia and Herzegovina,
[2] Faculty of Law for Economy end Justice, University Business Academy, Novi Sad, Serbia.

Abstract

This paper describes and analysis the attempt to introduce Internet governance as a special model against terrorist organizations, driven by increasing number of terrorist cells that use the Internet for the purpose of disseminating information, recruiting new members and communication in the preparation of their acts. This model of struggle is primarily related to: content control of Internet communications and efforts in passing legislation to place certain content on the Internet.

Key words: E- Government, Cyber terrorism, Geographical Location of The Software, Prevention of Terrorist Activities, Family.

1. Introduction

Establishment of a global government is a huge and complex thing, and therefore we can assume what is the complexity of setting up Internet governance. Efforts to try to pass laws on a global scale are the efforts that must include economic, cultural, developmental, legal and political interests of different states, the state association and the owners of multinational companies complicate further even in the area of computer systems. International terrorism via the Internet is a significant security issue which importance was highly understood on 11th September 2001. This terrorist attack, considering advances in information and communication technologies added new dimensions of this global problem. In newspapers and magazines, in movies and on television, in research and analysis, "cyber terrorism" has become a key word. In the year 1998 was formed an international organization ICANN (Internet Corporation for Assigned Names and Numbers), which is a non-profitable, public-private partnership company whose mission is to preserve the operational stability of the Internet.

From the time of ICANN, the debate about "Internet governance" is characterized by a number of government interference countries around the world, mainly through the United Nations. At the first World Summit of Information Society (WSIS), held in Geneva in December 2003 the question of "Internet governance" was on the session agenda of diplomatic representatives. Declaration of Principles and Action Plan adopted at the WSIS summit 2003rd, proposed a number of changes. When the term "Internet Governance" was presented at the WSIS Summit, many countries associated it to the concept of government.

One of consequence was the belief that the "Internet governance" should be primarily applied to the intergovernmental level, with limited participation and responsibility of certain individuals. The question is what was the main reason for this terminological confusion? Gelbestein and Kurbalija claim that to the most people term "Administration" means "government." They point out that the term "good governance" is used by the World Bank to promote the reform of the state, thus introducing more transparency, reducing corruption and increasing the efficiency of administration, taking action in the field of "Internet governance", including the establishment of the Working Group on "Internet governance" (WGIG)[1]. This was necessary because the terms "Internet" and "management" were the subject of controversial views, as was the concept of "Internet governance"[2]. The term "management" was a completely different perceived during WSIS summit. Poor understanding stemmed from confusion in terminology.

When the term "Internet Governance" was presented at the WSIS Summit, many countries related it the concept of government. One consequence of this was the belief that the "Internet governance" should be primarily applied to the

intergovernmental level, with limited participation and responsibility of certain individuals. The question is what was the main reason for this terminological confusion? Gelbestein and Kurbalija claim that to the most people to "Administration" means "government." They point out that the term "good governance" is used by the World Bank to promote the reform of the state, thus introducing more transparency, reducing corruption and increasing the efficiency of administration[3]. Based on the results we may consider these two authors that the term "administration" directly linked to key government functions [4].

Analyzing the concept of "Internet Management" by Robert Dahl in his article "Democracy and its critics" (1989), identifies the minimum requirements necessary to establish an efficient system of governance: government, law, sanctions and the judiciary.

Dahl believes that these four mechanisms form a "government" possible, i.e. government makes decisions about land management policy that complies with the judiciary, all in accordance with the legal framework and the implementation of sanctions on those who do not respect the laws [5]. Dahl's concept of "governance" is closer to the "government".

WGIG has published the following definition of Internet governance: "Internet governance is defined through the process of their development, implementation by Governments of the world, private sector and civil society, and through the use of shared principles, norms, rules and decision-making procedures and programs that shape the development and use of the Internet "[6]. This does not mean that the four above-mentioned mechanisms identified by Dahl, are not important because they occur in any discussion of the relationship between use of the Internet by terrorists and Internet governance.

2. Permeation of terrorism and the internet

in less than four weeks in April and May 2004., now deceased Abu Musab al-Zarqawi, who at one time was the leader of al-Qaeda in Iraq, attracted huge media attention, using a thoughtful combination of extreme violence and publicity on the Internet [7] . In early April 2004. Al-Zarqawi uploaded on the Internet audio recording that lasted for 30 minutes, explaining who he was, what he was fighting for and explained the details of the attack for which he and his group will be responsible.

Before this campaign encouraging speech on the Internet, the goal of each of the al-Zarqawi attacks was the killing of many people in order to emphasis the fact of the chaos and the large number of casualties in Iraq. The appearance to the public through the Internet, al-Zarqawi could control his statements about the actions of violence and to achieve greater media significance even with small operations.

In May 2004. Al-Zarqawi went a step further and published online video of decapitation of U.S. citizen hostage [8]. His aim was that through this image attract the attention of allies and enemies, which was undoubtedly successful. Al-Zarqawi risked very little on this occasion, but the effect was far greater than the killing of 100 people in Najaf, which made him a hero of jihad throughout the world [9]. The availability of this and other horrible videos on the Internet leads to the realization of the largest aspect of terrorism where terrorists use the Internet to exchange information and for recruitment needs.

"Jihad Warriors" effectively exploit the unique attributes of the Internet during the last five years. In fact, there are clear indications that the higher branches of Al-Qaeda cells that have formed special task exercise of protected communications in almost real time, to intense transmission of tactical and technical experience, as a medium for specialized training of its followers and the ideological propaganda of the possible successors.

In particular, the widespread use of this medium for command and control of the cell members to collect information on infrastructure facilities in a particular territory that could be targets of attacks. Internet has enabled the development of more independent and decentralized terrorist networks, which allows these networks to operate as a decentralized concessions or free agents (freelancers).

These networks allow terrorists to operate as a virtual transnational organization and reach out to their followers and sympathizers around the world, to maintain group identity, carry out and implement their indoctrination of ideology and principles (Gendron, 2007). Internet as a medium

spread uncensored information, regardless of their validity and potential impact. It allows even small groups to spread their message and exaggerate its importance and threats.

The militant groups are now active participants in numerous web sites. Many groups have shown they know how to use the power of the global information network for the purpose of the advertisement: Lebanese Hezbollah demonstrated this capability, and also the Tamil Tigers and al-Qaeda.

3. Content control problems

In case of detection of terrorist activities, national governments must play a major role in controlling the content on the Internet, which legally and lawfully have to be obtained by these countries. State agencies require operators of Internet content and what protocols should be controlled. Some groups or individuals, such as 'haktivists' on their own initiative omit the presence of numerous terrorist organizations on the Internet.

Therefore, the regulatory control of content and private initiatives require active or indirect participation of private companies, especially Internet service providers and companies that offer search services of Internet content, to which state and private organizations are pressing for regulating the content of terrorist organizations.

Here we must take into account the availability of appropriate technology to control content. General access control policy content has three Internet activities starting point: human rights (freedom of expression and right to communicate), government (legal control of the content) and technology (tools to control content). Freedom of expression and right of the user to claim, receive and give information is a fundamental right under Article 19 of the Universal Declaration of UN Human Rights (1948). On the other hand, this statement indicates that restricts the freedom of expression freedom in accordance with morality, public order and general welfare (Article 29). Therefore, the discussion on the implementation of Article 29 must be placed in the context of establishing a balance between the above views.

This dualism in acts of public international law on human rights opens the door to many opportunities for different interpretations of the norms regarding the right of speech. Control of content is limited to the interests of free speech and limit freedom of expression. Control of speech on the Internet is contrary to First Amendment law which guarantees freedom of expression, even the right of public expression of hatred and similar activities. Achieving an appropriate balance between content control and freedom of expression is a major challenge. Since the U.S. Congress seeks implementation of more stringent content controls, especially after 11. September 2001. The U.S. Supreme Court upholds the protection of the First Amendment.

Freedom of expression largely determines the position of the United States in international debates on the topic of "Internet governance". As long as the United States, as a signatory to the Convention on the Computer's Crime, distance themselves from the signing of the Additional Protocol which refers to criminal acts of a racist and xenophobic nature which are carried out through computer systems, the problem of hate speech over the Internet remains open [10]. In other words, while the Additional Protocol signed by the governments of the European Union and other signatory countries, where it is possible to add other statutes expression of hate crime, according to which terrorist groups and their supporters may be subject to prosecution, the same legal options do not exist in the legislation of the United States.

For this reason, many Internet sites of terrorist groups are located in the United States. For example, Internet service provider of Connecticut offered relocation services and virtual hosting for the website of the organization Hamas in the data center in Chicago and Connecticut. While Hamas Web sites were subject to observation only after 11 September 2001., Similar sites have been monitored in European countries before the event.

In 1997, appeared a controversial situation when it was discovered that the State University of New York (SUNY) hosted the web site of the Revolutionary Army of Colombia (FARC), a web site of the Revolutionary Tupac Amaru Movement Solidarity's hosted at the University of California at San Diego. SUNY shut down the official web site FARC, while San Diego has officially decided that for the freedom of speech stay on the server Tupac Amaru Web site a few years more. Many countries have access to technologies which it is

possible to prohibit dissent and limit the use of the Internet with. Successful use of the Internet for the recruitment of new members of terrorist organizations and other types of politic actions are based on the assumption that users have access to the Internet through which they exchange messages. Thus the state can limit their effectiveness by limiting access to Internet users, whether they actively censor any content on the Internet to control the infrastructure of the Internet, or to combine the preceding limitations.

The common element that is used for filtering index represents sites are blocked for access. If the web site listed here to access will not be allowed. Technically speaking, the filtering is done by using IP routing protocols, proxy servers and DNS redirection. Content filtering is done in many countries such as China, Saudi Arabia and Singapore, while other countries use censorship. For example, Australia has a filtering system for specific national web site, while the German states of North Rhine-Vestfalia requires Internet providers to filter access to most neo-Nazi sites. There are three types of Internet content filtering capabilities based on the content or a restraining order, which are discussed.

The first type consists of content where there is global agreement on the issue of control. Control the spread of child pornography over the Internet, is an area for which there is currently the largest consent. Although the guidance to terrorist acts and organizations of the same prohibited by international legal acts, in which there is general agreement about how to remove such content from the Internet, there are certain disagreements. The reason for this is that there is no globally accepted definition of terrorism, which makes things difficult. Consent, in that respect, is still possible to achieve as opposed to the creation of support in the fight against terrorism in any of its instances.

In terms of control, another type of content, which has been discussed, is content that may be sensitive to certain countries, regions or ethnic groups because of certain religious or cultural values. Ho most court cases refer to this type of content. Germany has a highly developed legal framework in this field and has experience in many cases against those responsible for hosting web sites with Nazi content. In France, Internet users denied access to one part of the Yahoo.com Web site in which they sale Nazi souvenirs. Most of the content control in Asia and the Middle East is justified for reasons of cultural and moral values. In this prohibition include: ban pornographic and gambling sites.

Finally we have a third type of content that is often discussed, which contains politically and ideologically sensitive material, which is one of censorship. There is a dilemma between the real and computer world. The existing rules on freedom of speech, which exist in the real world, can be implemented on the Internet. This is best explained within the European area, where, for example, decision-making framework for the EU Council on combating racism and xenophobia, to determine what is illegal in the real world is illegal and virtual [11].

Therefore, one of the arguments highlighted by those who believe that the Internet should have a specific legislation, tailored to its specific characteristics is that quantity (e.g. intensity of communication, the number of messages, etc.) makes a difference in quality[12]. Thus the problem of hate speech and terrorism is that it is not required for its suppression, but the fact that the spread of the Internet makes a distinction between terrorism and the spread of hatred on the Internet and its equivalents in the real world. Basically, most individuals are exposed to this type of hate speech and it is difficult to apply existing rules. Thus, differences within Internet are related mainly to problems of applying the rule, rather than the rule itself.

4. Position of U.S.A.

Immediately after the events of the 11. September, the FBI officially closed the hundreds, if not thousands of internet sites in the United States. For example, several radical Internet radio stations, such as IRA Radio, Al Lewis Live and Our Americas, the Internet service provider in Indiana eliminated after 11. September, while FBI warned them that they would be deprived of means for promoting terrorism. However, since these sites, which were shut down, did not directly encourage violence and collecting money, their shutting down was not in compliance with U.S. law and the increasing number of them was launched soon after they were turned off.

Of all the laws brought after 11. September, the most important in terms of Internet governance is the USA PATRIOT Act-2001., which declares illegal counseling or aiding terrorists, even through its Web site [13]. Babar Ahmad's case is interesting in this regard. Ahmad, who is a British citizen, was the founder of two well-known sites of jihad, and azzam.com and qoqaz.net, which are hosted in the U.S. and are the main suspects for raising funds for Islamist militants in Chechnya and elsewhere. The UK government has agreed to extradite Ahmad to the U.S. where Ahmad is serving a sentence for using the Internet for terrorist purposes [14]. Ahmad is not charged only for fundraising but also to encourage Muslims to "use all available resources to carry out military training and physical training for holy war" and giving "clear instructions" how to collect and direct funds, violent fundamentalist organizations through charity organization [15].

Similar charges, which Ahmad should be charged for, were brought against other U.S. citizens. However, due to the high level of protection of freedom of speech in the United States, at least two defendants were released without charges as follows: Sami Omas *Al-Hussayen*, a doctoral student of computer science at University of Idaho, who founded and maintained a radical web site, and Sami Amin al -Arian, a professor at the University of South Florida who was accused of publishing articles on violence committed by members of the Palestinian Islamic Jihad. The judicial process of Babara Ahmad will serve as another test of USA PATRIOT Act. It is obvious that Ahmed's case will be highly observed because of his speech on terrorism on the Internet in the United States.

5. Position of United Kingdom

Bombing in London on 7. July 2005. urged the British Government to participate in the struggle against terrorist Web sites inside and outside the UK. Immediately after the attack, State Secretary Charles Clarke in his speech in the lower house of parliament stressed the need to control the mechanisms of state power "those who incite terrorism, or ask others to support terrorist acts" [16]. In this speech, Clark emphasized that "the establishment of web sites or writing articles for the purpose of encouraging terrorism" activities that need to be controlled by this "new power". Draft Law on the Prevention of Terrorism Act of 2005. was close not to be adopted in Westminster in October 2005. Terrorism Act 2006, was introduced in the Parliament of the United Kingdom on 12 October 2005 and went into force on 30 March 2006 (http://www.opsi.gov.uk/acts/ acts2006/20060011.htm (7. 12. 2007.)). The opposition demanded two things:

- the new police forces have to hold suspects up to 90 days without charge,
- to punish "the encouragement or glorification of terrorism".

As for the "glorification of terrorism", such a measure would need to clearly criminalize the creation, maintenance and hosting numerous web sites that currently exist in the UK. The main criticism is that this provision may stifle legitimate political speech.

Several other measures were included in this bill, which could sanction the use of the Internet for the purposes of terrorism such as the work of preparing terrorist acts and terrorist training, are undoubtedly in the last parliamentary debates. This bill came into force in 2006.

6. International initiative

At the international level, the major initiatives are taken to control of content by European countries that have highly legalized speech of hate, and the European regional institutions try to impose the same rules in cyberspace. Key international legal instrument in terms of content control is Additional Protocol Treaty on Cybercrime of the Council of Europe. The protocol specifies the different types of hate speech that should be banned on the Internet, including racist and xenophobic materials, justification of genocide and crimes against humanity.

OSCE organization is also active in this regard. At the OSCE conference on freedom of media and the Internet in Amsterdam in June 2003 were adopted recommendations on freedom of media and the Internet. Recommendations to promote freedom of expression and the desire to reduce the censorship on the Internet in June 2004, the OSCE organized a meeting to discuss the phenomenon of interdependence racist, xenophobic and anti-Semitic propaganda on the Internet and hate crimes.

The focus of this event was a misuse of the Internet and freedom expression. These events provide a wider academic and political look at these aspects of control over content.

In May 2007. Ambassadors of the European Union agreed that the online portal known as the Check the Web, the European Police Office (Europol), should further strengthen the fight against terrorism. Web sites and content with chat communications that are subjects to control allow EU member states to collect data, sort them and form appropriate database of Islamist propaganda over the Internet.

Check the Web is only available to law authorities and experts, but the Safer Internet Action Plan has resulted in the establishment of the European network of hot lines, known as Inhope, which aim is to inform about illegal contents of the public. Today illegal content of pedophilia and child pornography are the most presented in the Internet.

7. Geographical location of the software

In the analysis of Internet governance, one of the key reasons for the debate was the fact that the decentralized nature of the Internet follows the application of excessive censorship. This is not true in every aspect, because it includes a number of techniques and technologies that provide effective control. From the technological point of view, control mechanisms can be avoided. In countries where government manages the control of content, technically experienced users find ways to circumvent such controls. It is still difficult to identify who exactly is behind a computer, but it is quite clear how to identify Internet service provider through which users access the Internet.

There are more recent legislation on electronic communications worldwide that require Internet providers to identify their customers and if required, to provide the necessary information to the competent authorities of the users. Many Governments have also plans to monitor users accessing the Internet from public places, particularly from Internet cafe. What is more represented in the Internet world, the less will be its unique "governance". For example, with the ability to geographically locate Internet users and their transactions, complex issues of legal competence can be solved more easily by existing laws.

One of the technological solutions aimed at detecting and preventing access to the content and messages inspirers and organizers of terrorist activities, the geographic localization of software, which identifies the location of computers and filtering access to certain Internet content according to national origin of computer. Case Yahoo! is very important in this regard, when a group of experts found that 90% of cases, Yahoo! could not determine whether some Web sites that advertise Nazi souvenirs, accessed from France.

This technological assessment helped the court to make a final decision. Companies that have the software for geographic location claim to be flawless to identify the country of origin and the city from which they accessed the Internet in 85% of cases, especially if it is a great city. Thus, such software can help Internet providers to filter Internet access, according to national origin and therefore to avoid court cases in foreign jurisdictions.

8. Hackers and haktivists

Events of the 11. September 2001. prompted a number of private companies and individuals on the Internet to find and destroy terrorist's Web sites.

Computer hackers have had a role in this type of activity. Shortly after the attack group, calling itself the "dispatching", followed by a posting that will destroy the web servers and Internet access in Afghanistan and other countries that support terrorism. This group was brought down thousands of web sites and launched a Distributed Denial of Service attacks (DDoS) attacks against various targets around the world, starting with the Iranian Interior Ministry and the Presidential Palace in Afghanistan. Do not provide all the support so-called hacker groups hacker war. German group of hackers "Chaos Computer Club" called upon all hackers, who took the law into their own hands, to stop their actions.

One of the reasons preventing the escalation of attacks may be that many hackers have been cautious about the negative associations with the terrorist attacks of 11 September, and they curb their activities. For the terrorist organization has never been easier to surf the Internet, even before the 11. September. Homepage of the site was the subject of alternate DDoS and other cyber attacks, and were also present and attacks on Internet service provid-

ers which caused numerous problems. For example, in 1997. bomb attack took place via e-mail that was directed at the Institute for Global Communications (IGC), Internet service providers in San Francisco, which hosted the website Basque separatist group ETA. The attack against IGC began after the attacks on ETA-known consultant in the north of Spain. The protesters wanted to put out the site on the Internet so it IGC finally removed from the server, but before that saved a copy of the site, allowing other providers to set up mirror-mirror sites, have appeared on dozens of servers on three continents. In addition, the campaign of anonymous e-mail haktivists sowed fear of a new era of censorship.

11. September 2001. established a number of official websites for the organization of monitoring terrorist Web sites. The most famous of these types of websites is the web site "Internet Haganah". Also known site of Washington DC's "Search for International Terrorist Entities" (SITE), which is like Internet Haganah focused on Islamist terrorist groups. Customers pay for services and use the SITE: FBI, U.S. national security and a number of media organizations.

Analysis of terrorist activities through the internet shows the duality of the Internet policy of Western states, primarily the U.S., compared to the website of Islamic extremists. On the one hand, induces the activity of hackers who exercise control and supervision on the internet, on the other hand the pressure is off and the physical Internet addresses terrorist organizations. A co-founder and director of SITE's Rita Katz has commented: "In our favor is going to exist as a terrorist sites run by companies in the United States. If the server is located in the U.S., then it goes in our favor when we need to monitor activities "[17]. Aeron Weisburd, who founded the Internet Haganah, said that his goal was to force the militants to move from one address to another: "Our goal is not to silence them, but to get them to move and communicate so they made a mistake, and we gather as much information about them at their every move "[18].

Supervision is done by downloading the entire traffic on the Internet with the help of certain people and software solutions. One way is by using the "digging through the data" for the detection of terrorist activities (using Data Mining for Detecting Terror-Related Activities on the Web)[19].

If there is evidence of terrorism on the Internet, Internet Haganah will contact the hosting company and ask them to remove the site from their servers. If this is done successfully, Internet Haganah will lease the domain name in the address would never be used again. Since its inception in the 2003[20]. Internet Haganah has merit in closing more than 600 sites that are linked to terrorism.

9. The role of families in the prevention of terrorist activities

Technology has obviously made the world smaller. The ability of technology that has revolutionized the economy and communications, has also encouraged many global terrorist potential, because with the help of electronic networks and highly developed technology, "wash" huge amounts of money, but also among other things, collect valuable "goods", ie. information.

It is evident that the obsession with Internet addiction is a growing problem. This problem is so pronounced that it became the practice, which began with the opening of the hospital, only to quit the Internet and video games. The first such hospital under the symbolic name of "Save the Brain" was opened in South Korea, which has an estimated two million drug users from the Internet. Bearing this in mind, particularly the alarming backlog of social problems and contradictions, and inability to respond to numerous challenges in a holistic front and in a comprehensive manner, increasingly turn to violence as a pillar that is basic cell of every society. Thus, the role of the family must be adapted in line with modern times in which we live, to expand to new modes of education, guidance and commissioning independent living children [21]. In addition, the importance of education and prevention of abuses in cyberspace, among other things, the dangers of terrorism in this virtual world, a necessary prerequisite for the formation of healthy and socially responsible person.

Worldwide known Islam followers believe that the obligation of the whole society, not only the state, is to address to the roots of such ideology which propagates terrorism. Obligations which have as an aim prevention activity of terrorism have a family, schools, youth organizations, social work services to religious com-

munities. The should make it more to do more to make up the roots of radicalism, extremism, if not eradicated completely, and it reduced the in order to then be turned into a purely into a safety issue.

For example, it is observed that the terrorists-suicide bombers can be said to come from religious families. They are very devoted to God and religion, and most attend Islamic religious schools. The most common are from the lowest social classes and the poor. Terrorist organizations are recruited through religious leader or a teacher, and today especially over the Internet. Interesting is the fact that among them there are highly different occupations.

The family must be encouraged to use the Internet adolescent controlled facilities in order to acquire new knowledge and new friendships regardless of their ethnic and religious affiliation [22]. The role of a family is of great importance in deterring children from monitoring sites with extremist's content. One must bare in mind the fact that adolescents aged 12-15 years are the most common target of these sites and they are most exposed to indoctrination by Islamist militant organizations. It must also be taken into consideration that most of the killed Jihad terrorists are minors, and therefore it follows that the role of families in the prevention of terrorist activities, primarily in terms of Internet terrorism decisive.

10. Conclusion

The chances for the emergence of the new 11. September are small in the near future, where the Internet has started to gain a new role since 2001. Terrorism and the Internet are significant global phenomena, which form various aspects of world politics. Due to its global presence and extensive multilingual context, it has the potential to impact differently on different types of politics and social relations. Unlike traditional mass media, the Internet's open architecture limits the efforts of the Governments of the world to regulate Internet activity, and this provides customers with enormous freedom and space to shape the Internet in their way.

The terrorists now know that a very clever use of traditional mass media, while also recognizing the value of direct communication channels. If terrorists want to send a message, they now have a chance to do it without action bombings and assassinations. Words are cheaper than life. The public does not see the terror, if they see that terrorists speak on television or the Internet, but they are scared if they see the victims of terrorist attacks, but not the terrorists [23]. Not everyone agrees with this statement. Over time, the state actors and individuals are trying to curb the occurrence of terrorist material on the Internet.

Authoritarian governments have had some success in using technology to restrict its citizens from accessing certain sites. There are a number of restrictive options in democratic countries, where although they adopted new restrictive laws in a number of judicial authorities, it remains unclear whether they will be effective as earlier attempts at control, such as cyber hate.

In terms of terrorist Web sites and their removal, private institutions, in cooperation with Internet providers are much more successful. However, the activities of individual activist seriously undermine freedom of speech and those who need to make decisions about these limitations. Such efforts may actually encourage us to think carefully about the legislation, not only in terms of setting up control, but also in terms of writing robust law of radical political speeches.

References

1. *WSIS Action Plan, World Summit on the Information Society, Geneva, 12 Decembar 03, document WSIS-03/GENEVA/DOC/5-E; www.itu.int/wsis/docs/geneva/official/poa.html, paragraph 13b.*

2. *Besic Carisa, Sedlak Otilija, Grubor Aleksandar, Ciric Zoran, "Measurement model for assessing the diffusion of e-business and e-marketing", TTEM journal, ISSN 1840-1503, 2011; 6(3): 651-656.*

3. *Milicevic Vladimir, Popovic Marko, Savic Zoran, "Business rule aproach as basis of e- bills payment system Development", TTEM journal, ISSN 1840-1503, 2011; 6(1):26-34.*

4. *Gelbstein Eduardo, Kurbalija Jovan , "Internet Governance: Issues, Actors and Divides", Geneva, Diplo Foundation and Global Knowledge Partnership, www.diplomacy.edu/isl/ig, 2005; pp. 10–12.*

5. *Klein Hans,"ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy", The Information Society, 2002; 18(3):194–195.*

6. *Report from the Working Group on Internet Governance, dokument WSIS-II/PC-3/DOC/5-E, 3 August 2005; paragraph 10.*

7. *Eedle Paul, "Al Qaeda's Super-Weapon: The Internet", International Conference "Al-Qaeda 2.0: Transnational Terrorism After 9/11", Washington, DC, 1–2 Decembar 2004.*

8. *Video "Abu Musab al-Zarqawi Shown Slaughtering an American"; www.globalsecurity.org/military/world/ para/zarqawi.htm.*

9. *Additional Protocol to the Convention on Cybercrime, Starzbur, www.conventions.coe.int/Treaty/EN/Treaties/Html/189.htm. 28. January 2003.*

10. *Proposal for a Council Framework Decision on Combating Racism and Xenophobia, Official Journal of the European Communities 2002/C 75/E17, 26 March 2002.*

11. *Petrović Slobodan R. ,,Kiber-terorizam - realnost ili fikcija?", Bezbednost, Beograd, 2000; 42(5-6): 643-675.*

12. *Bockstette Carsten, " Strategic communica-tions management techniques used by jihadi terrorists", Military Act, 2010 ; 62 (1): 326-353.*

13. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act). 2001.*

14. *United States of America v. Babar Ahmad and Azzam Publications, Indictment, United States District Court, District of Connecticut; www.usdoj.gov/usao/ct/Documents/AHMAD%20indictment.pdf.*

15. *"British Man Arrested on Several Terrorism-related Charges", Press Release, United States Attorney's Office District of Connecticut, www.usdoj.gov/usao/ct/Press2004/20040806.html. 6 August 2004.*

16. *Clarke Charles , "In House of Commons Debates", Hansard, 20 July 2005; 436: Column 1255.*

17. *Quoted in John Lasker, "Watchdogs Sniff Out Terror Sites", Wired News, 25 February 2005.*

18. *Bunt Gary, "Islam in the Digital Age: E-Jihad, Online Fatwas and Cyber Islamic Environments", London, Pluto Press, 2003; pp. 24 and 93.*

19. *Elovici Y. et al., "Using Data Mining Techniques for Detecting Teror – Related Activities on the Web", Journal of Information Warfare 2004; 3(1) : rr. 17-29.*

20. *Johnson Douglas B., Martin John. P. u Cyganov Viktor ,"Media-terrorizm:Terrorizm i sredstva massovoj informacyi", Nika-Centr, Kijev, 2004; pp. 20.*

21. *Geljman Marat , "Russkij sposob-Terrorism i mass-media v tretjem tysjachiletiyi", Guelman, Moskva, 2004.*

22. *Boccara Marie-Hélene, "Islamist Websites and Their Hosts Part I: Islamist Teror Organizations", MEMRI (The Middle East Media Research Institute),Washington D.C., 2004.*

23. *P. Alex, De Graaf Schmid and Janny, "Violence as Communication: Insurgent Terrorism and the Western News Media", London, Sage, pp. 170, 1982.*

Corresponding Author
Zaklina Spalevic,
Faculty of Law,
University Sinergija,
Bijeljina,
Bosnia and Herzegovina,
E-mail: zspalevic@sinergija.edu.ba