323.285:004

Fisnik Sadiku, MA[1]
Besnik Lokaj, MA[2]
Shpend Zogaj, MA (can.)[3]

NDIKIMI I TEKNOLOGJISË INFORMATIVE NË RRITJEN E TERRORIZMIT BASHKËKOHOR

ВЛИЈАНИЕТО НА ИНФОРМАТИЧКАТА ТЕХНОЛОГИЈА ВО РАСТОТ НА СОВРЕМЕНИОТ ТЕРОРИЗАМ

THE IMPACT OF INFORMATION TECHNOLOGY IN THE GROWTH OF CONTEMPORARY TERRORISM

Abstract

Imagine if information technology was not so highly developed, nor terrorism will be so widespread in size today. People have access to the Internet every day, they stay informed and keep in touch with family and friends via Internet and social networks almost every day, and so the terrorists stay informed and use these "benefits" that offers information technology. Use of information technology for terrorist purposes knows no national borders, and the potential impact on victims is very fast and on a large scale. Through this paper we will try to the reader to have a clearer understanding of the ways terrorist use information technology for their terrorist acts, and that the states that are not very developed, to enhance cooperation in the fight against this phenomenon and challenge. This paper first introduces the online terrorist propaganda and existing definitions of cyber terrorism and relevant terms. It clarifies the advantages that internet offers to terrorists. Then it

[1] Master in Security Studies, Pristina, Kosovo, fisniksadiku@gmail.com.
[2] Master in Security Studies, Pristina, Kosovo, besniklokaj@hotmail.com.
[3] Master (can.) in Security Studies, Pristina, Kosovo, shpend.pfsk@hotmail.com.

describes cyber terrorism as a new threat, how the terrorist organizations exploit cyberspace and why internet is an attractive choice for terrorists.

Key words: terrorism, cyberterrorism, internet.

Introduction

Technology, defined as the application of scientific knowledge to human problems, has contributed greatly to our ability to deal with situations in such a way as dramatically to alter the course of our existence and has challenged traditional state centric views of reality. It is modern technology to which we give credit for almost every improvement in medicine, nutrition, education, and our general standard of living. Technology has changed the nature of relations among nations and within them. Yet it is this same technology which has affected the nature of the life-threatening hostilities of the past century. As the most primitive weapons have been replaced with sophisticated, silent, and deadlier ones, technology clearly receives the credit[4].

Although terrorism knows no boundaries, as well as information technology, respectively Internet knows no boundaries. Everyone has access on Internet. The Internet can be used for good and bad purposes, as well as various illegal acts, including terrorism.

Terrorist and terrorist organizations stay informed via the internet. They use the Internet as a communication tool; tool for infiltration of new members through various propaganda; tool for achieving their medial goals to instill fear in the population worldwide, as well as a tool to execute attacks against networks, computer systems and communication infrastructure. All these are done to achieve their goals.

Theohary and Rollins has a similar thought, they say that the Internet is used by international insurgents and terrorist organizations as a tool for radicalization and recruitment, a method of propaganda distribution, a means of communication, and ground for training. Although there are no known reported incidents of cyber-attacks on critical infrastructure as acts of terror, this could potentially become a tactic in the future[5].While Wright notes that extremist groups use the Internet

[4]Bowers S, Keys K. Technology and Terrorism: The New Threat for the Millennium. *Research Institute for the Study of Conflict of Terrorism.* 1998; 65.

[5]Theohary C, Rollins J. Terrorist Use of the Internet: Information Operations on Cyberspace. *Congressional Research Service R41674.* 2011;2-4.

for many reasons: to disseminate propaganda and spread disinformation; to recruit and train volunteers; to solicit funds from sympathizers; to gather data from open sources; to plan and coordinate attacks; to maintain communications—many of them encrypted—between members of a single terrorist group as well as with members of other terrorist groups; to provide tutorials on building and planting explosive devices; and to publicize their acts of violence and ultimately enhance the perceived image of their great strength[6].

Almost everyone has the same opinion, but expressed differently. One for which we can say is that in addition to other means, the Internet has become a very powerful weapon for terrorist which in the past has made it difficult to measure the work of terrorists, but not their purpose. In addition, intelligence agencies and law enforcement agencies are doing a lot of work in front of the computer, to track and discover all that is stated above.

The Internet has opened global communication channels to anyone with computer access, creating a simple and cheap venue for spreading terrorist ideology. Interestingly, the regions with the largest concentrations of terrorist groups — the Middle East and Asia — have some of the lowest Internet usage rates. The highest rates are in developed countries, such as the United States, Canada, Australia and New Zealand[7].

Pages that are available to write in this paper, I don't want to use to give or cite various definitions of terrorism, since we all are witnessing the consequences caused by terrorist acts, and we all know what they are able to do, only to achieve their goals.

1. Online terrorist propaganda

Various terrorist groups today realize that targeting their enemies through physical violence, while influential, is not solely the best recourse to gaining an overall victory for their cause. Sophisticated terrorists such as Osama Bin Laden, realize that in initiating their terrorist campaign, which not only is patience a factor, but there is also a piece called propaganda that is heavily involved in the orchestration of

[6] Wright M. Technology and Terrorism: How the Internet Facilitates Radicalization. *The Forensic Examiner.* 2008. http://www.theforensicexaminer.com/archive/winter08/7/. Accessed February 6, 2016.

[7] Mantel B. Terrorism and the Internet. *SAGE Journals.* 2009; 129-153.

activities. Whether it is television, radio or the internet, terrorists realize that these instruments are valuable resources in instilling fear within a community or winning the hearts and minds of the populace[8].

Terrorists' use of social media has exploded over the past several years. Terrorist groups from ISIS to the Taliban use social media platforms to recruit, radicalize, spread propaganda and even raise money. Terrorists know the benefit of social media. Social media is easy to use, it is free, and it reaches everyone in the world. We have seen this most recently with the attacks in Paris; and after the attack, terrorists and their supporters took to social media to praise the attack, recruit new jihadists and fund-raise. Twitter has become one of the terrorists most popular platforms. As you can see here on the monitor—I believe we have the monitors ready—a British jihadi in Syria is bragging about ISIS and is threatening America. Some people make the excuse that there is no point in shutting down a social media account because it will pop again. But that is not always true. For years, Twitter was asked to shut down an account of the designated foreign terrorist organization, al-Shabaab, which pledged allegiance to al-Qaeda[9].

Regarding the Twitter platform, Turkey had condemned it due to terrorist propaganda, because in April 2015 had temporarily blocked Twitter and other social networks because of the publication of a picture in which an attacker puts a gun to the prosecutor's head that was killed in Turkey.

YouTube is a popular platform for jihadists as well. Videos are especially effective in attracting and funding and donations. Every major video released by al-Qaeda is uploaded to YouTube and, as soon as they are released, to jihadist forums. ISIS posts videos on YouTube in a service called Vimeo that depict graphic violence. However, YouTube does try to remove them but can't get them all[10].

Internet companies like Google, Facebook and Twitter are quietly stepping up their efforts to combat online propaganda and recruiting by Islamic militants by removing accounts that are suspected of being linked to terrorists. But even as many Internet companies become

[8]Lumbaca S, Gray DH. The Media as an Enabler for Acts of Terrorism. *Global Security Studies.* 2011; (2) 1: 45-54.

[9] Committee on Foreign Affairs. The Evolution of Terrorist Propaganda: The Paris Attack and Social Media. *U.S. Government Publishing Office: Washington.* 2015; 1-81.

[10] Ibid.

increasingly vigilant, they also worry that the public may see them as government tools and that technologically savvy militants will learn more about how to beat their systems. They also worry that they will face the same requests from countries across the world[11].

2. Advantages that internet offers to terrorism

As mentioned earlier, Internet access is easy from all. This access, gives to terrorists a big advantage, including faster communication between them, various planning, propaganda and hiding, and many other advantages that are dangerous for people, but also for national and international security agencies.

According to Tibbetts terrorist organizations also use existing Internet chat rooms and e mail to plan and coordinate operations. Many chat rooms are available for anonymous login, and can be accessed from cyber cafes, libraries or other Internet connections not traceable to a suspected terrorist group or member. Free e-mail hosting is also popular and available from a variety of sources. Not only do terrorist organizations use existing Internet services, they have constructed dedicated communications networks that utilize e-mail, the Internet and electronic bulletin boards (EBBs) to conduct seamless information processing and communications, both internal and external. When used in conjunction with any of a number of features available on the Internet -- anonymous mailers such as Send Fake Mail, or re-mailer utilities such as Jack B. Nymble -- email can be a powerful, responsive short-term tool to accomplish command and control tasks in a relatively secure manner[12]. While the U.S. Department of Homeland Security on its white paper noted that the terrorist groups are using the Internet to reach a much larger and more global audience than was possible just a decade ago. Some groups have rather sophisticated online presences, employing complex structures and hosting mechanisms, an array of multimedia platforms, and the use of logos and branding. Some groups are adapting to the Web 2.0 evolution, by utilizing online platforms that

[11] NBC News. Social Media Companies Move to Limit Terrorist Propaganda. http://www.nbcnewyork.com/news/national-international/Social-Media-Companies-Move-to-Limit-Terrorist-Propaganda.html. Published December 7, 2015. Accessed February 6, 2016.

[12] Tibbetts PS. Terrorist Use of the Internet and Related Information Technologies. *School of Advanced Military Studies, United States Army Command and General Staff College*. Fort Leavenworth, Kansas. 2001; 1-67.

are more interactive. They further point out that some terrorist groups have adopted the marketing strategy of "narrowcasting" their content to specific audiences. With youth, they target different age groups and focus the platforms, content, messaging, and appeal depending on age[13].

Digital camera, video cameras and various other technologies made it to individual consumers at an affordable price. As a result, terrorist groups no longer solely depended on news agencies. Not only could they produce their videos and forward them to news agencies, but with the invention of the internet, groups created websites that hosted their videos, publications, audio files, fundraising and various other materials that promoted their cause and attracted new recruits[14].

On the other hand, the MI5[15] Web site illustrates, the advantages of the Internet should not serve only terrorists but also those who confront them, not only in terms of monitoring and learning about terrorists but also in launching antiterrorism campaigns. For example, educational campaigns that encourage nonviolent forms for debate and teach conflict resolution techniques can provide a viable counterweight to terrorism campaigns. Web sites that expose the terrorists' lies and challenge their morally disengaged rhetoric can provide potential recruits with a logical analysis of a group's purported grievances and activities. Bearing in mind that terrorism is a war over minds and souls and that it often targets young people and children, Web sites can be particularly valuable in countering the insidious claims and arguments for terrorist organizations. A wide range of groups and organizations, from concerned citizens to NGOs and social organizations, can launch such alternative site and provide well-reasoned nonviolent voices[16].

According to this, as pointed out above in the last part, unfortunately in Kosovo eyes are only on Government and Law Enforcement Agencies. There is no initiative, or very little initiatives by citizens, civil society, and NGOs who have launched a campaign against violence, although religious communities have called for not joining terrorist

[13] The U.S. Department of Homeland Security. The Internet as a Terrorist Tool for Recruitment and Radicalization of Youth.*Homeland Security Institute.* White Paper.2009; 1-18.

[14]Lumbaca S, Gray DH. The Media as an Enabler for Acts of Terrorism.*Global Security Studies.*2011; (2) 1: 45-54.

[15] The Security Service (MI5) is a British Intelligence Agency.

[16]Weimann, G. *Terror on the Internet: The New Arena, the New Challenge.* United States Institute of Peace: Washington, DC; 2006:240.

groups. This situation becomes even more alarming, since it is known that since 2012 until now, the participant of Kosovars in the ISIS wars estimated 300 people. According to a report published by Kosovar Center for Security Studies[17]that despite Kosovo's backward economic development, poverty, and rural underdevelopment, the internet penetration rate and the number of internet users are among the highest in the region, and are comparable to many EU member states. The internet however, is a double-edge sword in the world of radical violent extremism; while it is useful for state authorities to track violent extremist groups, such groups also use the internet to recruit fighters from around the world. This report further notes thatEmotionally appealing videos posted online by ISIS propaganda tools have impacted a number of victims in Kosovo, resulting in many to leave their homes to join the conflicts in Syria, including those who previously practiced a more liberal form of Islam.

Besides propaganda on Internet and other negative issues or "advantages" that Internet and technology offers to terrorists, what is most worrying are bomb-making manuals. The possibility to obtain information via the Internet to construct explosive devices is not impossible. For example, a simple search on Google you can find a manual which is titled "Improvised Munitions Handbook: Improvised Explosive Devices or IEDs"[18]. Regarding the purpose and scope of this manual it states that the purpose of this manual is to increase the potential of Special Forces and guerrilla troops by describing in detail the manufacture of munitions from seemingly innocuous locally available materials. Further states that the manual contains simple explanations and illustrations to permit construction of the items by personnel not normally familiar with making and handling munitions. While this manual provides guidance for "not normally familiar with making and handling munitions", then my question would be what can make those who are "very familiar with making and handling munitions"?. Yazel- states that the availability of bomb-making information on the Internet should be a palpable concern for any lawmaker. Content that provides an "ingredient list" and instructions on how to make incendiary devices

[17]Kursani Sh. Report inquiring into the causes and consequences of Kosovo citizens' involvement as foreign fighters in Syria and Iraq. *Kosovar CenterforSecurityStudies*. 2015; 1-110.

[18]*See*: http://www.survivalcentral.net/wp-content/uploads/2011/02/improvised-munitions-army.pdf.

is presumptively more dangerous than other forms of violent content on the Internet. He further notes that information about constructing bombs is currently available in print[19].However, dissemination of bomb-making information in print comes with built-in barriers to access. Purchasing a bomb-making instruction manual requires many steps. First, those who search for information must locate a bookstore or publishing house willing to sell the information. Second, they must provide some form of payment for the materials. Third, they must be willing to bear the social consequences (whatever they may be) of purchasing a title that others frown upon. More importantly, each individual purchaser must incur all of these costs. The Internet substantially diminishes those barriers to information access[20].

The use of "how to" manuals for making bombs is not limited to isolated anecdotes. Federal courts observed the discovery of bomb-making manuals during investigations of several bombrelated crimes." Although possession of a bomb-making manual does not alone prove that a reader intends to commit an act of violence, both the Federal Bureau of Investigation (FBI) and the Bureau of Alcohol, Tobacco, and Firearms (ATF) "expect that because the availability of such information is becoming increasingly widespread, such bomb-making instructions will continue to play a significant role in aiding those intent upon committing future acts of terrorism and violence"[21].

3. Cyberterrorism as a new threat

Attacks that are launched over the Internet are commonly known as integral parts of what is commonly called "cyber-crime". Formerly,

[19]DEP'T OFJUSTICE, supra note 1, at 5. Publishing houses have produced titles such as THE ANARCHIST'S HANDBOOK (J. Flores, 1995), GUERILLA'S ARSENAL: ADVANCED TECHNIQUES FOR MAKING EXPLOSIVES AND TIME-DELAY BOMBS (Paladin Press, 1994), RAGNAR'S GUIDE TO HOME AND RECREATIONAL USE OF HIGH EXPLOSIVES (Paladin Press, 1988), and IMPROVISED EXPLOSIVES: How TO MAKE YOUR OWN (Paladin Press, 1985). Id. In considering whether mention of these titles in their report would bolster accessibility to them, the DOJ concluded that such information is "so readily available.., that [their] publication in a Report to Congress will create no additional risk." Id. at 32.

[20]Yazel BJ. Bomb Making Manuals on the Internet: Maneuvering a Solution through First Amendment Jurisprudence. *Notre Dame Journal of Law, Ethics & Public Policy*.2014;(16)1:281-284.

[21] Ibid.

perpetrators in this area were often young hackers, keen on experimenting with security-related issues and curious about technology. In the meantime, however, this situation has changed. Instead of experimenting youngsters, highly organized groups that use attacks as a source of income, businesses that conduct industrial espionage and states engaging in electronic warfare can be observed. The only group of actors that seem to be missing are the terrorists who rarely admit to computer-related aggression. Nevertheless, this is no reason for an all-clear. The events in Estonia in 2007, for example, have shown that even whole countries can be put at risk without the use of a single conventional weapon. This will not go unnoticed by terrorists. A more thorough look at the motivation of terrorists for attacks over the Internet is therefore of the essence before looking at the concrete possibilities for terrorist attacks[22].

According to Theohary and Rollins when terrorist groups do not have the internal technical capability, they may hire organized crime syndicates and cybercriminals through underground digital chat rooms. Reports indicate that terrorists and extremists in the Middle East and South Asia may be increasingly collaborating with cybercriminals for the international movement of money and for the smuggling of arms and illegal drugs. These links with hackers and cybercriminals may be examples of the terrorists' desire to refine their computer skills, and the relationships forged through collaborative drug trafficking efforts may also provide terrorists with access to highly skilled computer programmers[23].

Even Law Enforcement Agencies in Kosovo accept that this phenomenon remains a challenge for all security institutions, not only in Kosovo. Directorate against terrorism, in collaboration with the Unit of Cyber Crimes within the Kosovo Police, continuously monitors and tracks on the Internet, in order to identify the Web sites, portals or social networks, which propagate extremist ideology, or used to make calls or recruitment of individuals who are at risk of falling prey to this propaganda. Depending on the findings, they obtain the necessary actions, including the possibility of initiating criminal investigations and prosecutions, or even review of opportunities to take action limiting the

[22]Brunst PW. *A War on Terror: The European Stance on a New Threat, Changing Laws and Human Rights Implications.* Springer. 2012;52.
[23]Theohary C, Rollins J. Terrorist Use of the Internet: Information Operations on Cyberspace. *Congressional Research Service R41674.* 2011;2-4.

impact on society of these websites, portals or social networking accounts[24].

While regarding to international cooperation, plenty of investments have been made to prevent classical terrorist violence but the developed countries remain highly vulnerable to cyber-attacks against the computer networks that are critical to national and economic security. In order to protect their vital interests, many technology dependent countries concentrate on organizing their cyber security policies. Most of these nations have taken some sort of national legal and military measures. But without international cooperation, these national measures are inadequate against cyber terrorism. Regional partnerships also do not provide adequate cyber security, since the cyber-attacks can originate from off-region or off-partnership countries. In order to provide a worldwide international cooperation; the term "cyber terrorism" should be defined precisely and activities, considered as terrorist activity, should be determined as a first step. After that, developing both legislative and military collaborations should be discussed[25].

Our state also should be aware that this is very dangerous phenomenon and is not a myth anymore, but a reality for the international world as well as for our country.

4. Conclusion

States, despite the efforts to combat terrorism directly, should focus on preventing the spread of terrorism or terrorist ideas, especially those that are spread through the Internet and information technology. An important factor in this regard is the control of terrorist organizations for their actions on the Internet, which as we saw, can be a serious threat to the countries national security.

Based on a report by United Nations for Countering the Use of the Internet for Terrorist Purposes, is stated thatpreventing as well as investigating terrorist use of the Internet requires adequate legislation as well as effective technical solutions. The challenges presented differ

[24]KOHAnet. Shteti Islamik propagandon edhe në gjuhën shqipe. https://koha.net/?id=27&l=95311. Published January 25, 2016.Accessed January 26, 2016.
[25]Dogrul M, Aslan A, Celik E. Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism. *NATO Cooperative Cyber Defence Centre of Excellence.*2011 3rd International Conference on Cyber Conflict. 2011;29-43.

in important ways from those identified in the fight against more traditional terrorist activity. As a result of the available network technology and the multitude of Internet based services, these challenges range from preventing the availability of instructions on how to commit terrorist acts to monitoring the use of encryption technology in terrorist communications. While terms of the technical aspects, the report noted rapid developments in technology represent both a challenge and a tool for global efforts to counter terrorism. As terrorist groups turn to technical tools to organize, plan, run, finance and support their activities, their increasing reliance on technology also makes them vulnerable to government scrutiny. Governments are developing increasingly sophisticated techniques to identify and track potential terrorists.

List of references

Bowers S, Keys K. Technology and Terrorism: The New Threat for the Millenium. *Research Institute for the Study of Conflict of Terrorism.*1998; 65.

Brunst PW. *A War on Terror: The European Stance on a New Threat, Changing Laws and Human Rights Implications.* Springer. 2012;52.

Committee on Foreign Affairs.The Evolution of Terrorist Propaganda: The Paris Attack and Social Media. *U.S. Government Publishing Office: Washington.* 2015; 1-81.

Dogrul M, Aslan A, Celik E. Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism. *NATO Cooperative Cyber Defence Centre of Excellence.*2011 3rd International Conference on Cyber Conflict. 2011;29-43.

Kursani Sh. Report inquiring into the causes and consequences of Kosovo citizens' involvement as foreign fighters in Syria and Iraq.*Kosovar CenterforSecurityStudies*. 2015; 1-110.

KOHAnet. Shteti Islamik propagandon edhe në gjuhën shqipe. https://koha.net/?id=27&l=95311. Published January 25, 2016. Accessed January 26, 2016.

Lumbaca S, Gray DH. The Media as an Enabler for Acts of Terrorism.*Global Security Studies.*2011; (2) 1: 45-54.

Mantel B. Terrorism and the Internet.*SAGE Journals.*2009; 129-153.

NBC News. Social Media Companies Move to Limit Terrorist Propaganda. http://www.nbcnewyork.com/news/national-international

/Social-Media-Companies-Move-to-Limit-Terrorist-Propaganda.html. Published December 7, 2015.Accessed February 6, 2016.

Tibbetts PS. Terrorist Use of the Internet and Related Information Technologies.*School of Advanced Military Studies, United States Army Command and General Staff College.*Fort Leavenworth, Kansas. 2001; 1-67.

The U.S. Department of Homeland Security.The Internet as a Terrorist Tool for Recruitment and Radicalization of Youth.*Homeland Security Institute.* White Paper.2009; 1-18.

Theohary C, Rollins J. Terrorist Use of the Internet: Information Operations on Cyberspace. *Congressional Research Service R41674.* 2011;2-4.

Yazel BJ. Bomb Making Manuals on the Internet: Maneuvering a Solution through First Amandment Jurisprudence. *Notre Dame Journal of Law, Ethics & Public Policy.*2014;(16)1:281-284.

Weimann, G. *Terror on the Internet: The New Arena, the New Challenge.* United States Institute of Peace: Washington, DC; 2006:240.

Wright M. Technology and Terrorism: How the Internet Facilitates Radicalization. *The Forensic Examiner.*2008. http://www. Theforensicexaminer.com/archive/winter08/7/.Accessed February 6, 2016.