Chapter 3

Internet Forensics and Combating Terrorism

Krunoslav Antoliš [1]

Summary

Information technologies are an unavoidable and integral part of the lifestyle of a modern man who is using them fully aware of their usefulness, but frequently without enough information on the threats that directly endanger his own privacy in its narrower but also in its broader sense. In this respect, emphasis should be given to information on the threats accompanying information technologies, with particular attention being paid to the possibilities of the Internet abuse. The Internet as the communications platform of modern man is understood to contain the threat of identity theft, but our particular concern today is the abuse of the internet by terrorist, and primarily jihadist, elements.

The evidence indicates that violent jihadists use the Internet primarily to spread their terrorist ideologies and to encourage terrorist acts, and also as a platform for the recruitment and training of terrorists globally. During the preparation and terrorist attack stages, the Internet has additionally been used as communications infrastructure.

A particular, if at this stage potential, problem with the Internet is the prospect of Cyber terrorism. The (non-terrorist) cyber-attacks against Estonia, Georgia, and Kyrgyzstan illustrated the strength and power of such disruptive measures.

The issues which arise in the field of fighting terrorist Internet abuse are mainly of a legislative and then of an information technology nature, so it is necessary to make legislative and informatics *preconditions* for efficient combating terrorists by all those in charge of protecting us from the terrorists but also including ourselves.

Creation of a new information infrastructure and reinforcement of the existing one in which the Internet Forensics, as a growing discipline, will have a significant part, is not a small contribution to this struggle.

---

[1] Dr. Antolis is currently an official at the Ministry of the Interior of the Republic of Croatia, Police Academy, Police College, and is one of the original members of the Combating Terrorism Working Group.

Introduction

Ongoing global processes in the world today which have influence on the changes and development of strategic environment are primarily caused by strategic drives such as globalization, political geometry, demographic changes, environmental changes and the influence of new technologies and above all, the Internet.

According to the action and reaction principle, globalization has impact on overall world events, along with political geometry which from the view of partial transfer of sovereignty to the existing and newly-created alliances that go together with evident problems of the collapsed states and appearance of some non-state actors which are often the cause of non-conventional threats as well as the reason for coordinated response of the international organizations and security alliances.

One of the issues is the result of demographic changes and unwanted environmental changes such as global warming. The world is faced with the issue of energy resources regarding the location of the resources but also their supply routes as well as food and soon, water shortage. All previously mentioned is leading to poverty, hunger and diseases and humanitarian interventions and unavoidable migrations as an escape from the mentioned disasters.

New technologies, such as information and communications, biotechnology and nanotechnology and especially the Internet are among those that will also determine global processes and changes. It is their global impact that requires more detailed research along with the attention which should be paid to their abuse by the terrorists.

In the contemporary world information is the power. Therefore, information exchange is a process which directly influences the spreading of this power to all those that we are ready to share it with. One of the consequences of such global processes is establishment of new and preservation and spreading of the existing security alliances.

All those who can provide timely information by means of their own information resources, by bilateral and multilateral information exchange, will be able to prepare themselves for new security threats and challenges brought about by contemporary world processes.

Technical and Law Enforcement Pre-requisites in Fighting the Internet Abuse

In this respect, we should notice growing of new professional disciplines, which in time could become scientific disciplines such as the Internet Forensics. The Internet Forensics is comparatively little known discipline which appeared as a forensics discipline by gradually evolving from computer, i.e. network forensics. The Internet Forensics has moved the focus of attention of computer forensics from individual computers to the Internet. Internet Forensics is a global challenge of finding out the criminal activities and people behind those activities. The very term forensics is directly connected with the investi-

gations into *illegal* activities of individuals and groups and search for security solutions to overview and protection against the Internet threats, such as from a terrorist organization. Yet, just as in the case of computer forensics, different authors give different definitions of the Internet Forensics, some focusing on methodology deployed by the Internet forensicists, the others on the tools used by the Internet forensicists or on the purpose and reasons for applying the Internet Forensics. By its methods and techniques, the Internet Forensics is aimed at reinforcing our efforts in bringing to justice all those who are flooding us by spams or threaten by different forms of DoS (denial-of-service), DDoS (distributed denial-of-service), DRDoS (distributed reflected denial of service) attacks, etc., to our business activities done via the Internet. It is the Internet Forensics that will help us to discover the identity of the Internet thieves and create pre-conditions for bringing them to justice by means of digital forensics evidence collected from hidden places in emails, web pages, web servers and elsewhere on the Internet. The results obtained are very often used afterwards in building and/or upgrading the systems providing protection from similar threats in future.

To understand general threats coming from the sphere of terrorism, especially the information security-related issues, it is good to start from the wisdom of those who acquired it by considering the security issues seriously and systematically and writing some of it down in books such as "The Art of War" written by Sun Tzu. What I have in mind are the following quotations:

- "If you know the enemy and know yourself, you need not fear the result of a hundred battles."
- "So in war, the way is to avoid what is strong and to strike at what is weak."
- "Knowing the place and time of the coming battle, we may concentrate from the greatest distance in order to fight."
- "To win without fight is best."

If we agree with the thesis that the information means power then we certainly need to work out the protection of the systems which create, store, transmit and supply the authorized persons and those are the information systems as well as infrastructures which globally support them, that is, the Internet.

Strategic frame for combating terrorism is made through the National Strategy for Prevention and Suppression of Terrorism, the Republic of Croatia (Nn no.139 of 3rd December, 2008).

Croatia's legislative frame which secures protection of the information systems from terrorism and other threats includes also EU Convention on Cybercrime and the Information Security Act of 13th July 2007.

Amendments to the Penal Code and to the Criminal Procedure Act of 15th December 2008, based and adjusted to the EU Convention on Prevention of Terrorism, have also contributed to the quality of legal standards at the national level. For example, they introduce in criminal legislation of the Republic

of Croatia a new definition of terrorist act and criminal acts dealing with terrorism which include: recruitment and training for terrorism and public support to terrorism.

The Republic of Croatia, apart from national legislation in the domain of combating terrorism, has taken over the international responsibilities which are not small and include bilateral international cooperation in combating terrorism which is formalized by the treaties with 29 states including, first of all, the neighboring states. It also includes the responsibilities for multilateral cooperation and those taken over from the international organizations whose member state is Croatia, such as the UN, NATO and others, formalized in resolutions, conventions and protocols.

From the aforementioned, it is obvious that the terrorist act can be directly connected with the issue of the information security, i.e. that the information security can be threatened by a terrorist act. In this respect, it is important to study the relationship between the information security and terrorism with the aim to prevent and suppress unwanted situations caused by possible terrorist acts.

Terrorism – Yesterday, Today and Tomorrow

Contemporary terrorism is something essentially different from what we understood as terrorism before the events of 9/11/2001. Before 2001, terrorism was in service of the promotion of particular political options, parties, movements, states.

Yet, what terrorism brought us on 9/11 is the internationalization of the terrorist organizations which threatens global security and announces a new bipolarity.

The basic concept of this approach is a struggle which does not want, by means of terrorism, to reach the negotiation situations, new solutions and positions of those who use it, but a big global victory that will be spoken about and promoted through public meetings as well as by media, above all by the Internet.

But if we wonder what we can expect in the future, regarding a further transformation of the organizational form of the terrorist activities, which in accord with Sun Tzu teaching is good to be recognized, we can say that it is definitely a tendency to establish a Global Terrorist Movement (GTM), based on the "Global Jihad."

The claims on such tendencies and likely projects can be supported by some articles and books written by ideologists of terrorism, such as al-Suri's book "The Call for a Global Islamic Resistance," published in late 2004, in which the writer on 1600 pages analyzes the issue of jihad in order to justify and promote it.

However, the most recent research conducted by one of the biggest world centers for studying counterterrorism, the Combating Terrorism Center at West Point, the USA, have recognized the tendency and attempts of Al-Qaeda to reshape global terrorist movement. From the part of the conclusion of the re-

search entitled "Exploiting the Fears of Al-Qaeda's Leadership" by Associate Professor of Political Science and Director of Terrorism Studies at the Combating Terrorism Center at West Point, James J.F. Forest which says: "Al-Qaida operatives are persistent in reshaping global perception that they are a strong movement with cells worldwide," it is obvious that Al-Qaida really tends to be something similar to it, i.e., first to make an impression and then, most likely, to establish a global terrorist movement in future.

In any case, it is the right moment to find out, and act according to our national saying: There is no smoke without fire, or according to Sun Tzu's wisdom to spot a threat while still minor, to learn about it, and suppress it.

Unstable States and Terrorism

What we can expect to be the first target of the terrorist attacks are unstable states and their "recruiting" by various forms of force including financial one.

This is possible to expect since it is just the unstable states which are faced with serious economic, social and political difficulties, corruption and organized crime, ethnic and religious rivalry, human rights violation, suffering people, territorial disputes, inadequate or failed attempts to carry out reforms—e.g. non-transparent privatizations, dissolution of states and internal or interstate armed conflicts, active or frozen, a low level information safety—the main culprits are training, operational standards and international standardization.

What can be expected is financial expansion of the states whose capital supports the terrorists, especially towards the unstable states which we are currently faced with: financial overdebtness in the World Bank and other financial institutions of the developed states, corruption and organized crime – connected with the governing structures, non-transparent loan spending, etc. The only way for the country to survive or for the government to maintain power is to provide the money from the rough countries – at least temporarily, for what they are ready to make any concession to their saviors, including political one.

So, global financial crisis will certainly have impact on national, regional and global stability and be favorable for terrorism. It is clear that terrorists see it as their chance and talk explicitly through Al-Qaeda spokesperson Adam Gadahn who announced in a propaganda video of October, 2008 that this terrorist network was going to take advantage of financial crisis to give a decisive blow to "the enemies of Islam." Terrorism expert Bruce Hoffman says that Al-Qaeda's goal is to destroy the "Western lifestyle," "Al-Qaeda's propaganda in the past six years has stressed that that their goal is – our bankruptcy."

The Internet – Promotional, Educational and Recruitment Infrastructure of Terrorism

Media are the means particularly highly positioned in the terrorist concept with special emphasize on the Internet mainly due to the following features: decentralized infrastructure, easy access and anonymousness, global impact on the world public, fast communication, cheap maintenance and development of

web applications, multimedia possibilities, superiority over traditional mass media that search for information on the Internet when making news.

Yet, due to all the possibilities provided by the Internet and the central position it occupies in national information infrastructure, it should be adequately treated regarding the information security, especially ubiquitous terrorist abuse of the Internet.

The Internet abuse by the terrorist organizations is aimed at creating publicity and propaganda as a form of psychological war in the service of networking, recruiting and mobilization via the Internet forums and similar, data mining of the targets and information exchange, for example about manufacturing of the improvised explosive devices (IED) and providing the means to manufacture them, fundraising for donations, planning and coordination along with preservation of secrecy by coding the messages and communications, for public provocation to commit a terrorist offence.

Frightening is the data obtained through the research project at University of Arizona's Artificial Intelligence Lab Chen's "Dark Web," that there are 500000000 terrorist pages and reviews on the Internet today, tens of thousands of them about IED explosive devices.

Concern over the information security threat by terrorists at global, regional and national levels is clear and justified. Very likely and relatively simple to be carried out, the information threat by cyber terrorism is recognized globally by the largest states such as the USA , Japan and others and security alliances such as NATO. In this respect, European states are not less threatened, so it is important to point out their reorganization in the domain of combating cyber terrorism. For example, the German military (Bundeswehr) is training their own hackers to defend themselves from denial-of-service attack.

How big the threat is coming via the Internet regarding encouragement of terrorism is obvious from the invitation to the BH Muslims for the "duty of jihad" which was announced on the Internet portal www.putvjernika.com, on 14th February 2009, being the third serious Internet invitation to BH Muslims in the Bosnian language to join the terrorist actions on the portal registered in the US state of Ohio.

Generally, reviews of the terrorist pages are focused mainly on the following topics: historic development of organizations, list of their activities, terrorist actions, their attitude to social and political issues, biographies of prominent members, information on ideological goals, explicit recognition of the adversaries and their criticism, some web pages include description or video recordings of violent activities of Hezbollah and Hamas and even the handlers of suicide bombers.

Great attention is directed to the target groups: current and potential supporters, sympathizers, international public opinion, special emphasize is on interaction with journalists and multilingual approach to the contents, to the enemies, their demoralization and creation of the sense of guilt undermining in this manner the support of the public to the governments of the adversary

states, making internal enemies in the adversary states, i.e. making pre-conditions to establish GTM.

It is possible, for example, to find a terrorism recruiting manual on the Internet in which the authors Brian Fishman and Abdullah Warius teach how to radicalize and organize new generations of terrorist operatives. The 51-page-long manual Abu 'Amr al-Qaidi "A Course in the Art of Recruitment," is made to enable less trained jihadists for recruiting entirely independently and be successful in recruiting secular and modest Muslims into the Jihadist movement.

Since global recession is favorable to various types of extremism, western countries will not be spared, either. So, the US Department of Homeland Security stresses that their problem is rightist extremism. In their opinion, rightist extremists in the USA could take advantage of the economy recession and the election of the first president of African origin to recruit new members. What is also favorable to the rightist extremists are the forced sales of the houses and apartments, unemployment and insolvency which might create a fertile soil for recruiting that sort of extremists.

War veterans could become recruiting targets thanks to their war experience, particularly those who have problems with returning to civil life. Also, new regulations proposed on carrying and possessing arms could cause discontent among the members of the rightist organizations. At the same time, some conservative commentators criticized these warnings claiming that it was the case of criminalization of political discontent of the citizens and suffocating the freedom of speech.

Conclusion

Despite many legal provisions which today enable the establishment of a high level of information security, one part of the information infrastructure still remains in the legal and formal vacuum, and that is the Internet. The Internet may have no boundaries, but law enforcement does. All of the use of the Internet by terrorists that we see today is not possible to easily prevent due to its global character, and the non-existence of global and generally accepted legal norms to regulate the Internet. Such norms should have an international character – at the level of UNSC resolutions, conventions or protocols, and would apply the same standard to everything that is accessible via the Internet. All the above-mentioned points are the grounds to start the initiative to establish the International law of the Internet – similar in nature to the International Law of the Sea. Namely, just as the sea is global, the ubiquitous dimension of the Internet is global, too. But unlike the sea, the Internet washes all the world states; there are no countries without an Internet "coastline." These Internet norms should be observed by the states that host the Internet providers, first of all regarding their authority and responsibilities for monitoring the contents and services and then the authority to react and sanction.

This effort represents a major legal challenge to the international community and, at the same time, if effective legislation can be agreed on, would provide a major contribution to combating global terrorism, especially concerning

the terrorist abuse of the Internet which is a worldwide battlefield of ideas, aimed at establishing a transnational terrorist movement. The complexity of this demand starts from the legal requirement of maintaining an admittedly difficult balance between democratic freedom and the restriction of absolute freedom on the Internet, in order to prevent and suppress the advantages that this means of communication provides terrorist adherents on a daily basis.

References

1. Abu 'Amr al-Qa'idi, *A Course in the Art of Recruitment*, http://revolution.thabaat.net/?p=964.
2. Krunoslav Antoliš, "Information & Organization Prerequisites for Combating Terrorism," *Vojaškošolski zbornik*, no.4 (December 2005): 51-65.
3. Krunoslav Antoliš, Presentation at CTWG conference, PfP Consortium, 14-17 November 2004, Oberammergau, Germany.
4. Krunoslav Antoliš, "Prerequisites for Systematic Fighting Terrorism," *Croatian International Relations Review* XI, no. 40/41 (July/December 2005, Zagreb, Croatia): 121-125.
5. Krunoslav Antoliš, "The National Strategy for the Prevention and Suppression of Terrorism," *Police & Security*, CODEN POSIE9, No. 1/90 (January/February, 2009), Zagreb, Croatia, pp.150-153.
6. Michael Chertoff, "5-year Terrorism Threats Forecast for U.S.," www.msnbc.msn.com/id/28387496.
7. James J.F. Forest, "Exploiting the Fears of Al-Qaeda's Leadership," http://ctc.usma.edu/default.asp.
8. Thomas Frank, "Feds consider searches of terrorism blogs," www.usatoday.com/news1/washington/2008-12-23-terrorblogs_N.htm.
9. John Goetz, Marcel Rosenbach, and Alexander Szandar, "National Defense in Cyberspace," www.spiegel.de/international/germany/0,1518,606987,00.html.
10. Michael Lipin, "Al-Qaeda Seeks to Capitalize on Global Financial Crisis," www.voanews.com/english/archive/2008-11/2008-11-21-voa3.cfm?CFID=176543362&CFTOKEN=41072727&jsessionid=663020f2a6352b17c1a936233246256a1650.
11. Brent MacLean, "Terrorism and Internet Use," www.canadafreepress.com/2007/internet-security092107.htm.
12. Sun Tzu, *The Art of War*, www.chinapage.com/sunzi-e.html.
13. Gabriel Weimann, "How Modern Terrorism Uses the Internet," The United States Institute of Peace, www.usip.org/pubs/specialreports/sr116.html.
14. The map of United states of Islam, http://littlegreenfootballs.com/weblog/?entry=14952&only

15. A Jihadist's Course in the Art of Recruitment, http://revolution.thabaat.net/?p=964.
16. US Officials, "Recession Could Fuel Right-Wing Extremism," By *VOA News*, 15 April 2009, www.voanews.com/english/2009-04-15-voa27.cfm.
17. National Strategy for Prevention and Suppression of Terrorism of the Republic of Croatia, Nn no. 139, 3 December 2008.
18. EU Convention on Cybercrime, Nn no. 09/2002.
19. EU Convention on Prevention of Terrorism, Nn no. 10/2007.
20. The Information Security Act, Nn no. 79/2007.
21. Amendments to the Penal Code and to the Criminal Procedure Act, Nn no. 152/2008.