Information & Security: An International Journal

Vase Rusumanov, v.34:2, 2016, 137-150 https://doi.org/10.11610/isij.3409

THE USE OF THE INTERNET BY TERRORIST ORGANIZATIONS

Vase RUSUMANOV

Abstract: Human life progress has successfully defined multiple epochs' evolution with specific peculiarities. Today we live in the modern digital era, numerous computer devices, services and networks are actually significant. At the same time, these new science and technology achievements are rated both as good and bad for their users. The digital progress is however visible and of utility for terrorist organizations. This article focuses on selected illustrations of Internet technologies used by terrorist organizations. Special discussion emphases are given to uses towards (i) terrorist organizations radicalization of young people; (ii) spreading propaganda; (iii) internal communication, training, planning, coordination and committing terrorist acts.

Keywords: terrorism, cyberterrorism, terrorist organizations, Internet, cyber attacks, propaganda, communication.

Introduction

Today, at a time when it is challenging to make war between powers with different militarily potential, new methods of asymmetric warfare are being developed. The modern battlefield is already in the cyberspace, implementing different weapons: logical bombs, DDoS, Trojan horses, worms, rootkits, viruses, social engineering, etc.[1]

This new cyber war, practically contributes to everyday life digital systems terminating, spying, information compromising or manipulating. Unfortunately, this science and technology achievements are also used by terrorist organizations, which with the help of the new cyber weapons, the Internet and smart environment of living can practically compromise most of the modern critical infrastructure components. For instance, attacks like overloading communication lines, water supplies pollution, confusions of traffic controls, modifying manufacturing process know-how, energy lines and power plants intrusions, stock market sabotages, etc.[1]

The story of the terrorist groups' presence in cyberspace has barely begun to be told. In 1998, less than half of the 30 organizations designated as Foreign Terrorist Organizations maintained websites. By the end of 1999, almost all 30 terrorist groups had established their presence on the global network. Today in the era of Web 3.0, all active terrorist groups are establishing at least one form of presence on the Internet. A quick outlook on the Internet shows thousands of websites, social network profiles, online forums and chat rooms serving terrorists and their supporters.[2]

Therefore, there are multiple reasons of the modern cyber terrorists' actively to use the Internet environment: [3]

- *easy accessibility*: anyone can have an Internet access from anywhere, either on a land-line or on radio or satellite connection or through WLAN net-works. This way, for instance one can get access to the Internet even from the desert;
- *the rules are minimal, there is no censorship:* this is well perceptible from debates going on nowadays about how the Internet could be regulated, thus preventing the spread of the objectionable web sites;
- *the target audience is potentially huge:* access to the given content is unrestricted, the number of those getting access is affected only by the capacity of the server or the bandwidth;
- *anonymity of communication:* due to the problem of detectability it is not known who is communicating with whom at the given time;
- *information flow is very fast:* as soon as a web page is prepared, it is put on the Internet and from that moment on it is accessible to anyone;
- *its formation is very cheap, it does not require big costs:* its infrastructural background that has to be provided only once, which, from that moment on, can be used freely;
- *multimedia environment:* in which possibilities are given (audio, video, image, text) by which deterrence, propaganda, etc. can be made to a significant extent;
- *traditional mass media regards the Internet as its source more and more:* they often refer to the various Internet news portals.

Terrorism and the Internet

Looking at the Internet presence of a certain modern terrorist organization one can see that most on the websites are presenting the history and activities, the main goals for achievement, biographies of the leaders, founders, and heroes, fierce criticism of the enemies, and up-to-date news. Terrorists are targeting for their sites, visits mostly by: [4]

- *Current and potential supporters*. Terrorist websites make heavy use of slogans and offer items for sale, including T-shirts, badges, flags, and video-tapes and audiocassettes, all evidently aimed at sympathizers. Often, an organization will target its local supporters with a site in the local language and will provide detailed information about the activities and internal politics of the organization, its allies, and its competitors.

- *International public opinion*. The international public, who are not directly involved in the conflict but who may have some interest in the issues involved, are courted with sites in languages other than the mother tongue. Most of the sites offer versions in several languages. ETA's site, for instance, offers information in Castilian, German, French, and Italian. Whereas, the MRTA site offers Japanese and Italian in addition to its English and Spanish versions; and the IMU site uses Arabic, English, and Russian. For the benefit of their international audiences, the sites present basic information about the organization and extensive historical background material (material with which the organization's supporters are presumably already familiar). Judging from the content of many of the sites, it appears that foreign journalists are also targeted. Press releases are often placed on the websites in an effort to get the organization's point of view into the traditional media. The detailed background information is also very useful for international reporters. One of Hezbollah's sites specifically addresses journalists, inviting them to interact with the organization's press office via email.
- *Enemy publics*. Efforts to reach enemy publics (i.e., citizens of the states against which the terrorists are fighting) are not as clearly apparent from the content of many sites. However, some sites do seem to make an effort to demoralize the enemy by threatening attacks and by fostering feelings of guilt about the enemy's conduct and motives. In the process, they also seek to stimulate public debate in their enemies' states, to change public opinion, and to weaken public support for the governing regime.

How Terrorists Use the Internet

Exploring possible ways for terrorists' use of the Internet, an aggregation on several key moments, such as: planning and execution of terrorist acts, spreading propaganda, recruiting new members, finding financiers, training its members, communication etc.,[5] will be further discuss in details.

Communication

One way of using the Internet is for communication between the members of the terrorist organization. It is known that Osama bin Laden had communicated with Al Qaeda with laptop and wireless network via encrypted messages.[1] Thereby, encryption is a way of protecting the messages from unwanted reading. In this way unauthorized reading or changing of messages could be achieved. The level of protection depends from the encryption algorithm complexity. Two crypto techniques – symmetric and asymmetric are basically used nowadays. The symmetric technique implements one and the same key for both encryption and decryption, while in the asymmetric one – two different, but related keys (public and private) are used for encryption and decryption.[6]

Members of terrorist organizations communicate with each other using different servers that are available online. They often communicate through emails using different free email service such as Yahoo, Gmail etc. Characteristic for this mode of communication is that terrorist organizations have provided a way to remain anonymous and their conversations can't be monitored by the intelligence services. Thus, in order intelligence services to follow certain people and their communication it is necessary to have communication between different emails.

The organizational structure of the terrorist organizations is always in function of goals of the organization, i.e. represents the most appropriate, simple mechanism to operate. The activity of terrorist organizations is conducted according to a program document in which ideologist, creator and organizer of terrorist actions suggests the goals, which should be achieved with their activity. Military - political command is established in certain bigger cities which represent branches and independent military and political units. All larger and well-organized terrorist organizations have well-established hierarchical network and the basic unit called the “cell.” It is a miniature, much efficient organizational unit, which usually has five to ten people, but there are cases, depending on the action, to be consisted of more people. Each “cell” has a conspiratorial name for recognition and identification with other cells of the terrorist organization. The communication with the higher units is commonly realized through courier, telephone connection, and now more recently, is very often usage of the Internet and the opportunities it offers to us. Because of conspiracy, usually one of the lower organizational units knows only one of the higher organizational units.[7]

The terrorist organizations communicate without being monitored in that way that few members have a common email of which they know the username and the password of this email. This email they use in that way that the members do not send the message to another email address, but the message they want to send to the other members they write and save in the folder “Drafts”, without sending to another email address.[1] When other members want to read the message, they sign in the e-mail address, entering the username and password and go to the folder “Drafts”, where the message is saved. This is now the most common way that terrorist organizations avoid the surveillance by the intelligence services, and the probability of being detected is in fact small, because intelligence services have to know the exact address, username and password through which such communication takes place. Another way of communication that is used by the terrorist organizations is communicating via encrypted messages on the various Internet forums, where the terrorist organizations in the form of encrypted text left the message to its members. The encrypted message can be publicly read. For understanding the meaning of the message, it is necessary that the members of the terrorist organization to have a ‘book’ with the codes to be able to decrypt the messages.

Promoting Actions and Goals

The work of the terrorist organizations is very important to be promoted, noting: ideas, goals and actions that they may take. Their main objective is audience, not victims.[8] Most of the terrorist organizations have their own websites, however there are such that do not have, and are using the web pages of other terrorist organizations. In this way one may find out evidences for terrorists, concerning: organization independent acts, supported acts by other terrorist organizations and partnering activities with other larger organizations.

Terrorists Talks on Internet

Many of the websites or social networks profiles connected to certain terrorist organizations are posting speeches by terrorist leaders or other members of the higher structures of their organizations. In these speeches a rhetoric that justifies positively the use of force for different ultimate goals (e.g. religious, political, ideological or ethnic superstition) achieving is mostly represented. At the same time, these leaders are constantly keeping the side of peaceful resolution of disputes. They are noting, at the same time, on those who are fighting against their beliefs and values reluctance for resolving these problems peacefully. In these speeches is also represented a rhetoric for heroic freedom fighters’ achievements, fulfilling and respecting their rights and values in contrast with those who are fighting against. Emphasize is also given to their weakness and at the same time innocence, complaining that organizational members and followers are prosecuted, arrested, tortured and harassed. Terrorists are hoping in this way to spin the truth and represent themselves as victims of other people views and actions.

ISIS propaganda uses four main themes to encourage young people to travel to Syria and Iraq. These themes are used to recruit both men and women, and are also widely used in discussion on the social media around ISIS. ISIS celebrates and promotes an image of success online in order to attract young people – it tells them that ISIS are the winning side and can offer them an exciting life. The ISIS slogan ‘Baqiyah wa-Tatamaddad’ (remaining and expanding) presents the group as one that consistently achieves success. ISIS propaganda ignores the reality that ISIS is not winning and is opposed by the majority of people in Syria and Iraq. ISIS portrays their ‘Caliphate’ as an ideal, utopian state where Muslims will find status and belonging. ISIS propaganda claims that it is the duty of Muslim men and women in the West to travel there and regularly states that all foreigners are welcome in its ranks, so long as they are Sunni Muslims. In reality the claimed Caliphate has been rejected by the overwhelming majority of Islamic scholars around the world. ISIS abuse of women and children and killing of innocent civilians has been well documented. The propaganda output of ISIS insists that it is the personal duty of Muslims to support them and travel to the 'Caliphate'. Islamic scholars have clearly dismissed this and have made clear there is no such obligation. ISIS wants to portray itself as the only group able to defend Sunnis from the Assad regime, the Iraqi army or the threat of the West. ISIS communications also provide food and services to people in Syria and Iraq. In reality, most Sunnis fear and oppose ISIS and recognize that they are a threat to their lives and security.[9]

Moreover, the speeches of the members of ISIS is evident the Islamic terminology, to reinforce the impression that it is fighting for a religious cause and has established a truly Islamic state. Terms used in ISIS propaganda and by supporters on social media includes: [9]

- Dawla/Dawlah – A term used to describe ISIS by its supporters, an alternative to "Islamic State";
- Caliphate – A Caliphate (or Khilafah) is a form of government used by early Muslims, under a single leader, or Caliph. ISIS supporters describe the territory the group controls in Iraq and Syria as the "Caliphate";
- Jihad – Literally meaning "struggle" jihad can also refer to violence. Extremists may claim that undertaking violent jihad is obligatory for Muslims;
- Mujahid – Someone who fights jihad, the plural of which is mujahideen;
- Hijrah – Referring originally to the journey made by the Prophet Muhammad and his followers from Mecca to Medina, today hijrah is used by many to mean moving from a non-Muslim country to a Muslim country. ISIS uses this term to reinforce the idea that there is a religious obligation to travel to their so-called Caliphate;
- Shahada – This can refer both to the Islamic declaration of faith (the first of the five pillars of Islam) and to someone considered to have achieved martyrdom. In this case they will be referred to as a "Shaheed";
- Kaffir/kuffar – A pejorative term used to describe non-Muslims, on the basis that they reject the tenets of Islam;
- Ummah – This is the concept of the world community of Muslims, who are bound by common faith. ISIS regularly makes claims to be representing the "one true Ummah" and that it is building a community for them;

- Rafidha – The Arabic word for “rejecters” or “those who refuse”, it is a term used to describe those believed to reject Islamic authority and leadership. “Rafidha” is often used by ISIS supporters as a pejorative or sectarian term against Shia Muslims;
- Sham – A classical Arabic term used to describe the region of the Levant, largely focused on Syria.

Radicalization of New Members

When we talk about the term “radicalization” we must say that there is no generally accepted definition in academia and government. The history of the concept of “radicalism” can offer some guidance as to what should be a defensible under-standing of the term “radicalization”. Today, the term “radicalization” has different meanings. To illustrate how academics define the term “radicalization,” some definitions from different authors will be chronologically given:

- *Ongering* (2007): “process of personal development whereby an individual adopts ever more extreme political or politic-religious ideas and goals, becoming convinced that the attainment of these goals justifies extreme methods”;[10]
- *Ashour (2009):* “Radicalization is a process of relative change in which a group undergoes ideological and/or behavioural transformations that lead to the rejection of democratic principles (including the peaceful alternation of power and the legitimacy of ideological and political pluralism) and possibly to the utilization of violence, or to an increase in the levels of violence, to achieve political goals”;[11]
- *Sinai (2012):* “Radicalization is the process by which individuals – on their own or as part of a group – begin to be exposed to, and then accept, extremist ideologies”;[12]
- *Schmid* (2013): “an individual or collective (group) process whereby, usually in a situation of political polarization, normal practices of dialogue, compromise and tolerance between political actors and groups with diverging interests are abandoned by one or both sides in a conflict dyad in favour of a growing commitment to engage in confrontational tactics of conflict-waging. These can include either the use of (non-violent) pressure and coercion, various forms of political violence other than terrorism or acts of violent extremism in the form of terrorism and war crimes. The process is, on the side of rebel factions. Generally it is accompanied by an ideological socialization away from mainstream or status quo-oriented positions towards more radical or extremist positions involving a dichotomous world view. And the acceptance of an alternative fo-

> cal point of political mobilization outside the dominant political order as the existing system is no longer re-cognized as appropriate or legitimate.[13]

Previously, if terrorist organizations had to build strategies and seek ways to come into contact with people and to radicalize their views and activities; today they have a useful tool - the Internet. With the help of the Internet, the terrorists today can easily act on the mentality and the views of the people and to radicalize them. In a few seconds they can put their speeches, photos, videos on the Internet and vast number of people who use the Internet can read, hear and watch all those materials that are intended for radicalization.

Some groups have established websites designed specifically for youth audiences, disseminating propaganda and radicalize through colourful cartoons and games. These sites – many of which are available in English – help to get the groups' message out to a worldwide audience, including any young person that has access to an Internet connection. In recent years, there have been reports of a growing trend by which young persons have the potential to self-radicalize through the use of the Internet. In 1998 there were a total of 12 active terrorist related. By 2003 there were approximately 2630 sites, and by January 2009 a total of 6940 active terrorist-related websites.[14] Today, the number of web sites related to some terrorist organization is much bigger. Another case to note of self-radicalisation is Irfan Raja, who was a 19-year old British student whose "entire radicalisation occurred online, with hours spent online downloading extremist videos, posting messages, and chatting with other radicals."[15] In 2007, Raja made contact with an extremist recruiter online and, along with four other young British persons he had never met, prepared to travel to a training camp overseas.

Additionally, it's evident that Islamic terrorist groups have revealed video games online to appeal to teens and young adults. Hezbollah released the games "*Special Force" and Special Force 2*", which depict themselves fighting the Israeli military. The Global Islamic Media Front, in association with Al Qaeda, released the "Quest for Bush game" online. The game, aimed at children, giving them a goal of killing the President George W. Bush.[16]

ISIS is one of the terrorist organizations which use the social media to radicalize new members. One of ISIS's more successful ventures is an Arabic-language Twitter application called The Dawn of Glad Tidings, or just Dawn. The application, an official ISIS product promoted by its top users, is advertised as a way to keep up on the latest news about the jihadi group. Hundreds of users have signed up for the application on the web or on their Android phones through the Google Play store. When you download the application, ISIS asks for a fair amount of personal data. Once you sign up, the application will post tweets to your account—the content of which is decided by someone in ISIS's social-media operation. The tweets include links, hash-tags, and images, and the same content is also tweeted by the accounts of everyone else who has signed up for the application, spaced out to avoid triggering Twitter's spam-detection algorithms. Your Twitter account functions normally the rest of the time, allowing you to go about your business.[17]

Financing

On the Internet they found potential supporters of their ideology and goals that are ready to finance terrorist organization, in order to fulfil previously set goals. Like many other political organizations, terrorist groups use the Internet to raise funds. Al Qaeda has always depended heavily on donations, and its global fundraising network is built upon a foundation of charities, non-governmental organizations, and other financial institutions that use websites and the Internet based chat rooms and forums. The Sunni extremist group Hizb al-Tahrir uses an integrated web of the Internet sites, stretching from Europe to Africa, which asks supporters to assist the effort by giving money and encouraging others to donate to the cause of jihad. Banking information, including the numbers of accounts into which donations can be deposited, is provided on a site based in Germany. The fighters in the Russian breakaway republic of Chechnya have likewise used the Internet to publicize the numbers of bank accounts to which sympathizers can contribute. Such bank accounts are located in Sacramento, California. The IRA's website contains a page on which visitors can make credit card donations.[2]

Planning

Many terrorist organizations in its operation use computer systems and the Internet to plan their activities, i.e. for planning and execution of certain terrorist acts.

Al Qaeda operatives relied heavily on the Internet in planning and coordinating the September 11 attacks.[18] Thousands of encrypted messages that had been posted in a password-protected area of a website were found by federal officials on the computer of arrested Al Qaeda terrorist Abu Zubaydah, who reportedly masterminded the September 11 attacks. The first messages found on Zubaydah's computer were dated May 2001 and the last were sent on September 9, 2001. The frequency of the messages was highest in August 2001. To preserve their anonymity, the Al Qaeda terrorists used the Internet in public places and sent messages via public e-mails. Some of the September 11 hijackers communicated using free web-based e-mail accounts.

Hamas activists in the Middle East, for example, use chat rooms to plan operations and operatives exchange e-mail to coordinate actions across Gaza, the West Bank, Lebanon, and Israel. Instructions in the form of a maps, photographs, directions, and technical details of how to use explosives are often disguised by means of steganography, which involves hiding messages inside graphic files.[3]

Since 9/11, US sources have monitored several websites linked to Al Qaeda that appear to contain elements of cyber planning (directions for operatives, information for supporters and activists, call for action, threats and links to other websites): [3]

- *alneda.com*, which US officials said contained encrypted information to direct Al Qaeda members to more secure sites, featured international news on Al Qaeda, and published articles, fatwas (decisions on applying Muslim law) and books;
- *assam.com*, believed to be linked to Al Qaeda (originally hosted by the Scranton company BurstNET Technologies, Inc.) served as a mouthpiece for jihad in Afghanistan, Chechnya and Palestine;
- *almuhrajiroun.com*, an Al Qaeda site which urged sympathizers to assassinate Pakistani President Musharraf;
- *qassam.net*, reportedly linked to Hamas;
- *jihadunspun.net*, which offered a 36-minute video of Osama bin Laden;
- *7hj.7hj.com*, which aimed to teach visitors how to conduct computer attacks;
- *aloswa.org*, which featured quotes from bin Laden tapes, religious legal rulings that “justified” the terrorist attacks, and support for the Al Qaeda cause;
- *drasat.com*, run by the Islamic Studies and Research Centre (which some allege is a fake centre), and reported to be the most credible of dozens of Islamist sites posting Al Qaeda news;
- *jehad.net*, *alsaha.com*, & *islammemo.com*, alleged to have posted Al Qaeda statements on their websites;
- *mwhoob.net* & *aljehad.online*, alleged to have flashed political-religious songs, with pictures of persecuted Muslims, to denounce US policy and Arab leaders, notably Saudi.

Training

Many terrorist organizations use the Internet for training its members or persons who support their ideas and goals. On many of the sites that are controlled by the terrorist organizations is shown how to make bombs, explosives, how to prepare certain toxins, how to execute a particular terrorist act, etc. “The Terrorist’s Handbook”[18] and “The Anarchist Cookbook”[19] are two well-known manuals that offer detailed instructions on how to construct a wide range of bombs. Another manual, “The Mujahideen Poisons Handbook”,[20] written by Abdel-Aziz in 1996 and “published” on the official Hamas website, shows how to prepare various homemade poisons, poisonous gases, and other deadly materials for use in terrorist attacks. A much larger manual “The Encyclopedia of Jihad”[21] and prepared by Al Qaeda, runs to thousands of pages; distributed through the Internet, it offers detailed instructions on how to establish an underground organization and execute attacks. Another manual is “Sabotage Handbook”,[22] which is used from Al Qaeda and published through the Internet. In this manual is shown how to plan assassination and anti-surveillance methods. One example is the deadly bomb attack in Finland, 2002. For months, the brilliant chemistry student who called himself RC had been discussing bomb-making techniques with other enthusiasts on a Finnish Internet Web site devoted to bombs and explosives. Sometimes he posted queries on topics like manufacturing nerve gas at home. Often, he traded information with the site’s moderator, who used the screen name Einstein and whose message carried a picture of his own face superimposed on Osama bin Laden's body, complete with turban and beard. Then he set off a bomb that killed seven people, including him, in a crowded shopping mall. The Website used by RC, known as the Home Chemistry Forum, was shut down by its sponsor, a computer magazine called Mikrobitti. Yet a backup copy was available with postings by teenagers who used names like Ice Man and Lord of Fire, was immediately posted again, on a read-only basis.[23]

Execution

The terrorist organizations are also using the Internet for the execution of the terrorist acts. For example, explicit threats of violence, including in relation to the use of weapons, may be disseminated via the Internet to induce anxiety, fear or panic in a population or subset of the population. In many Member States, the act of issuing such threats, even if unfulfilled, may be deemed an offence.[24]

Additionally, they use the Internet for committing cyber attacks. A cyber attack generally refers to the deliberate exploitation of computer networks as a means to launch an attack. Such attacks are typically intended to disrupt the proper functioning of the targets, such as computer systems, servers or underlying infrastructure, through the use of hacking, advanced persistent threat techniques, computer viruses, malware, flooding or other means of unauthorized or malicious access.[25] Cyber attacks may bear the characteristics of an act of the terrorism, including the fundamental desire to instil fear in furtherance of political or social objectives.

An example of a cyber attack was seen in Israel in January 2012, targeting of multiple symbolic Israeli websites, such as the websites of the Tel Aviv Stock Exchange and the national airline, and the unauthorized disclosure of the credit cards and account details of thousands of Israeli nationals.[25] While a considerable amount of attention was focused in recent years on the threat of cyber attacks by terrorists, that topic is beyond the scope of the present publication and, as such, will not be a subject of analysis.[25]

Conclusion

Evidently with the modern world digitalization most of the societal functional mechanisms in various fields of life are constantly changing. The Internet services are adding great benefits and opportunities in facilitating these. Today, we communicate online with other people all over the world, exchanging: messages, videos, music, photos, reading news, blog posts, watching movies, playing games, collecting information about different topics of interest, using distributed software solutions, services and resources for our problems solving and sharing at the same time common emotions, values and rights.

All these are gain from the digital technologies, in many cases, are abused and instead of being constructive are controversially involved into destructive activities. With the advent of the digital era the regular use of computer systems, mobile devices, connected via the Internet, new security challenges are constantly emerging.

Todays' digital world provides terrorists with cheap and flexible communication, implementing free and anonymous web pages, e-mails and crypto services, fake blogs and social network profiles or even damaging gamming avatars. Additional propaganda and social engineering is also successfully organized in this environment. The promotion of radical ideas, goals and actions for installing fear and radicalism among the young people is constantly growing, producing terrorist active followers and sympathizers. They are also initiating numerous cyber attacks, targeting mostly important infrastructural facilities in this context.

Meanwhile in their operations, the terrorists are actively using Internet also for financing, planning, organizing and executing distributed attacks. Taking also the advantages offered by free software solutions of leading web services providers. Apart of these, the providers in themselves are trying to support the governmental officials and intelligence services in countering such events, producing a new asymmetric cyber war.

Finally, because of the active dual role of modern technologies it is necessary to establish relevant cyber strategies, policies and measures for combating these new security challenges. This idea could also benefit from the development of regional and international cooperation initiatives, exchanging of best practices, organizing joint counterterrorist operations and training, providing a better understanding of both technological and legal joint necessities.

Notes:

[1] Mina Zirojević-Fatić, "Abuse of Internet for terrorist purposes," *International Problems* 63, no. 3 (Belgrade: Institute for International Politics and Economy, 2011): 417-448 (in Serbian language).

[2] Gabriel Weimann, "How Modern Terrorism Uses the Internet," Special Report (Washington DC: United States Institute of Peace, 2004), p. 2.

[3] Zsolt Haig and László Kovács, "New Way of Terrorism: Internet and Cyber-terrorism," *Aarms Security* 6, no. 4 (2007): 659–671.

[4] Gabriel Weimann, "How Modern Terrorism Uses the Internet," Special Report (Washington DC: United States Institute of Peace, 2004).

[5] United Nations Office on Drugs and Crime, *The Use of Internet for Terrorist Purposes* (New York: United Nations, 2012).

[6] Depavath Harinath, M.V. Ramana Murthy, and B. Chitra, "Cryptographic Methods and Performance Analysis of Data Encryption Algorithms in Network Security," *International Journal of Advanced Research in Computer Science and Software Engineering* 5, no. 7 (2015): 680-688.

[7] Zlate Dimovski and Ice Ilijevski, *International Terrorism* (Skopje: Grafortrans, 2011).

[8] Brian Michael Jenkins, *International Terrorism: A New Kind of Warfare* (Los Angeles: Crescent Publication, 1975).

[9] "How social media is used to encourage travel to Syria and Iraq briefing note for school," Home Office, Department for Education United Kingdom, 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/440450/How_social_media_is_used_to_encourage_travel_to_Syria_and_Iraq.pdf.

[10] Alex P. Schmid, "Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review," Research Paper (The Hague: International Centre for Counter-Terrorism, 2003).

[11] Omar Ashour, *The De-Radicalization of Jihadists: Transforming armed Islamist Movements* (London: Routledge, 2009).

[12] Joshua Sinai, "Radicalization into Extremism and Terrorism," United States, *Intelligencer: Journal of U.S. Intelligence Studies* 19, no. 2 (2012): 21-27.

[13] Alex P. Schmid, *Glossary and Abbreviations of Terms and Concepts Relating to Terrorism and Counter-Terrorism* (London: Routledge, 2011).

[14] Gabriel Weimann, *The Internet as a Terrorist Tool to Recruit Youth* (Arlington, VA: Youth Recruitment & Radicalization Roundtable, 2009).

[15] Peter Neumann and M. Brooke Rogers, *Recruitment and Mobilization for the Islamist Militant Movement in Europe* (London: King's College for the European Commission, 2007).

[16] Andrew Kaczynski, "8 Ways Terrorists Use the Internet for Recruitment", *BuzzFeed News*, April 22, 2013, http://www.buzzfeed.com/andrewkaczynski/8-ways-terrorists-use-the-internet-for-recruitment.

[17] J.M. Berger, "How ISIS Games Twitter: The Militant Group That Conquered Northern Iraq Is Deploying a Sophisticated Social-media Strategy," *The Atlantic*, June 16, 2014, http://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/.

[18] *The Terrorist's Handbook*, 2005, http://www.dvc.org.uk/cygnet/tthb.pdf.

[19] William Powell, *The Anarchist Cookbook* (New York: Barricade Books, 2002).

[20] Abdel – Aziz, *The Mujahideen Poisons Handbook*, 2004, https://www.oodaloop.com/wp-content/uploads/2015/03/Mujahideen-Poisions-Handbook.pdf.

[21] Alexei Malashenko, Stephen R. Bowers, and Valeria Ciobanu, *The Encyclopedia of Jihad*, Faculty Publications and Presentations (Liberty University, Helms School of Government 2001).

[22] The US Department of Justice, *The Sabotage Handbook*, 2001, http://www.justice.gov/sites/default/files/ag/legacy/2002/10/08/manualpart1_1.pdf.

[23] Gabriel Weimann, "Virtual Terrorism: How Modern Terrorism Uses the Internet," *Journal of International Security Affairs*, 2007.

[24] United Nations Office on Drugs and Crime, *The Use of Internet for Terrorist Purposes*, (New York: United Nations, 2012): 11.

[25] Isabel Kershner, "Cyberattack Exposes 20,000 Israeli Credit Card Numbers and Details About Users," *New York Times*, January 6, 2012, http://www.nytimes.com/2012/01/07/world/middleeast/cyberattack-exposes-20000-israeli-credit-card-numbers.html.

About the Author

Vase RUSUMANOV holds a Bachelor of Criminalistics and is doing a Master in the field of criminalistics at the Faculty of Security – Skopje. He works in the Ministry of Interior of the Republic of Macedonia, and a Founder and President of the Research Centre for Security, Defence and Peace – Skopje. His research interests are in the field of terrorism, counter-terrorism, narco-terrorism, cybersecurity, organized crime, illegal trafficking, intelligence and counterintelligence.