Proceedings of Papers

2-nd International Scientific Conference MILCON'19, Skopje

«‹›»MILCON'19«‹›»
INTERNATIONAL SCIENTIFIC CONFERENCE
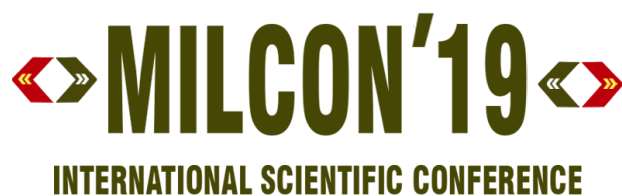
November 12th, 2019

MILCON 2019 International Scientific Conference is supported by:

This conference is organized under scientific auspices of the following institutions:

The Conference is organized by the Military Academy "General Mihailo Apostolski"- Skopje associated member of the University "Goce Delcev" - Shtip, within the RADLI Project (Regional Advance Distributive Learning Initiative), supported by the Kingdom of Norway and implemented by the Jefferson Institute, USA.

The Conference has been immensely supported by the Ministry of Defence and the Armed Forces of the Republic of North Macedonia

Preface

Respected readers,

In front of you is the thematic Proceedings, as a collection of papers presented at the 2nd MILCON'19 Conference "Contemporary education based on ADL", organized on November 12th 2019, by the Military Academy "General MihailoApostolski" - Skopje associated member of the University "Goce Delcev" - Shtip, within the RADLI Project (Regional Advance Distributive Learning Initiative), supported by the Kingdom of Norway and implemented by the Jefferson Institute, USA.

The objective of the Conference was to gather educators and trainers from different countries in order to give us the opportunity to increase both knowledge and cooperation within all aspects of advance distributed learning - ADL. Hence, the Proceedings contain **32** papers focused on the contemporary trends in the use of information technology in a pedagogical way, as well as the best practices both from a theoretical point of view, but also from a practical aspect on the topics related to educational programs using blended learning, emerging learning technologies, multiplatform delivery of courseware, motivational and pedagogical learning strategies and other topics related to ADL. This international scientific conference gives us a wonderful opportunity for exchanging experience and knowledge between the scientific workers and the practitioners from North Macedonia, USA, Serbia, Poland, Slovenia, Bosna and Hercegovina and Norway.

The papers published in the Proceedings are written by eminent scholars as well as by members of the security system participating in the educational process of the army, police and other security services from different countries.

Each paper has been reviewed by international experts competent for the field to which the paper is related.

The data and information gained with the empirical research, as well as theoretical thoughts and comparative analyses in the Proceedings will give a significant contribution to the development of the use of ADL in a pedagogical way.

We wish to extend our gratitude to all authors and participants to the Conference, as well as to all those who contributed to, or supported the Conference, especially the Kingdom of Norway and the Jefferson Institute, as well as to the Ministry of Defense and the Armed Forces of the Republic of North Macedoniafor their immense support of the Conference.

Skopje, November 2019

Conference chairs

JUGOSLAV **ACHKOSKI**
North Macedonia

BILJANA **KAROVSKA ANDONOVSKA**
North Macedonia

Keynote Speakers

AARON **PRESNALL**
USA

TONY **MULLIS**
USA

GEIR **ISAKSEN**
Norway

PIOTR **GAWLICZEK**
Poland

International Scientific Committee

GEIR **ISAKSEN**
Norway

DARKO **ŠČAVNIČAR**
Slovenia

NEVENA **SERAFIMOVA**
North Macedonia

BILJANA **PRESNALL**
USA

NEVEN **TRAJCHEVSKI**
North Macedonia

AARON **PRESNALL**
USA

ORCE **POPOVSKI**
North Macedonia

TONY **MULLIS**
USA

METODI **HADZI-JANEV**
North Macedonia

SAE **SCHATZ**
USA

STOJCE **DESKOVSKI**
North Macedonia

PIOTR **GAWLICZEK**
Poland

SIME **ARSENOVSKI**
North Macedonia

SEAD **MURATOVIC**
Bosnia and Hercegovina

GORAN **SHIMIC**
Serbia

BEKIM **MAKSUTI**
North Macedonia

DEJAN **RANCIC**
Serbia

VLADMIR **TRAJKOVIK**
North Macedonia

Organizing Committee

SLAVKO **ANGELESKI**
North Macedonia

DRAGE **PETRESKI**
North Macedonia

ROSE **SMILESKI**
North Macedonia

ZORAN **JOVANOVSKI**
North Macedonia

METODIJA **DOJCHINOVSKI**
North Macedonia

SASHO **GELEV**
North Macedonia

ZORAN **GACOVSKI**
North Macedonia

ALEKSANDAR **GLAVINOV**
North Macedonia

NENAD **TANESKI**
North Macedonia

TONI **GEORGIEV**
North Macedonia

ANDREJ **ILIEV**
North Macedonia

LAZAR **GJUROV**
North Macedonia

OLIVER **ANDONOV**
North Macedonia

ALEKSANDAR **PETROVSKI**
North Macedonia

SASO **DANEVSKI**
North Macedonia

ELENIOR **NIKOLOV**
North Macedonia

JONCHE **IVANOVSKI**
North Macedonia

MILCON 2019 Reviewers

SASHO **GELEV**
North Macedonia

PIOTR **GAWLICZEK**
Poland

SEAD **MURATOVIC**
Bosnia and Hercegovina

NEVENA **SERAFIMOVA**
North Macedonia

AARON **PRESNALL**
USA

BILJANA **PRESNALL**
USA

NEVEN **TRAJCHEVSKI**
North Macedonia

NENAD **TANESKI**
North Macedonia

ELENA **TRAJANOVSKA**
North Macedonia

JUGOSLAV **ACHKOSKI**
North Macedonia

TONY **MULLIS**
USA

LAZAR **GJUROV**
North Macedonia

ZORAN **GACOVSKI**
North Macedonia

SLAVKO **ANGELESKI**
North Macedonia

DEJAN **RANCIC**
Serbia

GEIR **ISAKSEN**
Norway

BILJANA **KAROVSKA ANDONOVSKA**
North Macedonia

ANDREJ **ILIEV**
North Macedonia

ELENIOR **NIKOLOV**
North Macedonia

GORAN **SHIMIC**
Serbia

JOVAN **BAJCETIC**
Serbia

ALEKSANDAR **PETROVSKI**
North Macedonia

Conference Secretariat

ELENA **TRAJANOVSKA**
North Macedonia

ANER **BEHLIC**
Bosnia and Hercegovina

BILJANA **DULOVIC**
Montenegro

KRISTIJAN **ILIEVSKI**
North Macedonia

Contact Information:

✉ *milcon@mod.gov.mk*

📞 *+38971292498*

Modern platforms on the Internet as a instrument of power in hands of violent religious extreme organization

N Taneski[1], B Karovska-Andonovska[2], A Petrovski[3]

[1,2,3]Military Academy "General Mihailo Apostolski", Goce Delchev University, ul. Vasko Karangelevski b.b, 1000 Skopje, North Macedonia

E-mail: nenoreal@yahoo.com, biljanakarovska@yahoo.com, aleksopetrovski@gmail.com

Abstract. A massive and wide acceptance and use of social networks by side of global religious extremist militant organizations has a major impact on the spread of international terrorism and is a growing threat to international security. When it will be in the hands of violent religious extremist militants personified in terrorist organizations, is a strong driver for indoctrination and attracting followers, profiling targeted groups, fundraising, to placing the instructions and guidelines for the development of weapons and actions in certain situations. Modern platforms on the Internet expressed through social networks represent ideal tools for processing information with the aforementioned objectives, expressed through text, photographs, audio, and video. So far, despite the fact that many measures have been taken to define the rules for the use of social networks against the promotion of terrorist and extremist groups, there are still many difficulties in the efforts to implement these measures due to the inability to track real-time information for a large number of information generated by users. Defining and specifying the concept and purpose of social networks, allows us to perceive the opportunities for their use.

1. Introduction

After the collapse of the bipolar system of international relations, modern terrorism expressed through the action of global religious extremist organizations is the greatest current threat to the modern world. Modern international terrorism, as a phenomenon, is a complex form of organized, individual and rarely institutionalized political violence. Over the last decade terrorism has evolved and has become an essential threat to international security.

This evolution reflects the ability to use modern technologies and tools that further enrich its complexity, dynamism intensity, but also its enormous danger to national security of states and to overall international security. The evolution of international terrorism is particularly due to its presence in cyberspace, which is mostly expressed by using social networks as a tool for acting in the pursuit of "higher goals".

2. Information as an instrument of power

Modern society, whose contemporaries we are, is critically dependent on information as a strategic resource and the information and communication technology that transmits, processes and exchanges them. Modern warfare is unthinkable without a lot of information about the opponent, their own forces, space and time. However, in addition to the advantages they provide, information has become an important goal for the opponent. To deprive the opponent of the advantage that it gives, while securing the necessary information for own needs, means to achieve a significant advantage in the realization of the purpose of a certain space and for a certain time with minimal engagement of forces and minimal losses.

The modern armed forces largely rely on the latest technological advancements in the field of communication and information technologies. The Information Revolution transforms the war, that is, causes changes in how societies come into conflict and how their armed forces lead the armed conflict. No more massive army forces are fighting against bloody exhausting struggles. Instead, small and

exclusively mobile forces, "armed" with real-time information, with high speed hit unexpected places. The winner is the one who can use the information faster, that is, the one that he / she can quickly analyze, assesses the situation and react. Major changes occur in how information is collected, stored, processed, taught and displayed, and how organizations themselves are organized to use the increased volume of information. Information becomes a strategic resource. Domination in the information spectrum is a necessary condition for success and victory in the conflict. The information environment in which the information acts as a power tool is divided into three components: physical part, contents of the information, and knowledge.

The physical part is even more commonly known as the "Cyber Space", which includes means and ways of connecting and the way of information delivery. This section covers information infrastructures, various communication lines (wired and wireless), computer networks, etc. Cyber space is the universe of computer networks, a world in which multinationals, societies and other subjects struggle to capture data and information. By "cyberspace" is meant "a kind of community" comprised of networks of computers where the elements of classical society are in the form of bits and bytes, that is, space created by computer networks. All of this previously mentioned interconnectedly represents a unique physical space covering all segments of the mainland, the sea, the air, and the universe. In a modern society of global connectivity, a conversation or a million-dollar transaction are made between people from one end of the world, quickly and cheaply.[1]

Computer networks allow people to create a whole range of new social relationships in which they can meet and influence each other. Thousands of groups can be formed to discuss various topics, play games, entertain each other, and even work on complex collaborative projects. Cyberspace is a "house" for thousands of groups of people who meet to share information, discuss common issues, practice work. The content of the information covers everything that is transmitted, whether it is text, images, databases, video. Knowing as a third segment of the information encompasses the impact, ie the perception that the content of the information has on the target audience.

This segment of the information environment is produced projected behavior of a particular target group or groups of recipients of the information, or the desired effects of the information creator are achieved. And precisely this piece of information as an instrument of power is a powerful tool in the hands of religious extremist organizations to achieve their goals. The information has the power to indoctrinate and attract sympathizers to a particular cause across the globe, as will be seen from the examples given below in this paper. The information has the power to force financial resources in support of the realization of the goals of the organization. And in the end the essential power is in the message it conveys with the content itself, which for religious extremist organizations, especially the Islamic State, is the cruelty with which it opposes its opponents. It can be concluded that in the modern existence of information technology and information-dependent planet, information as an instrument of power expressed through its content in the infinity of the cyberspace is a powerful tool for shaping world trends and attitudes, as well as for attracting followers for certain massive movements and causes, which are largely in favor of the survival of international religious extremist organizations.

3. Online radicalization

Online radicalization is described as a specific social environment that shapes the culture, behavior and symbols of individuals, groups, social networks and relationships, through which these individuals and groups develop and appear. The researcher Peter Waldman assigns various and independent qualities to this online environment, portraying them as social entities with their own right, which is a collective of people who share certain views and a unitary identity: "subculture" or "community". This does not mean that the conflict is absent in any of the online radicalization and violent religious extremist groups that emerge from them. Online radicalization has its own interests that lead not only to connect but often to criticize, and sometimes even to confront their violent individuals and cells. Perhaps most importantly, Wildldon's concept of online radicalization promotes that they are not only social relations as essential characteristics, but necessarily implicitly or explicitly is the interaction between persons who are radically online.[2] The advent of the Internet (Web 2.0) has allowed religious extremist organizations the opportunity to transform their widespread

online presence in expediently interactive extremist action and radicalization.[3] Osama bin Laden's cadres used the Internet for communication and propaganda purposes before the September 11, 2001 attacks in the United States, but their use of the Internet exponentially increased after attacks. This is due to two related reasons: 1). The loss of the al-Qaeda base in Afghanistan and the subsequent disintegration of its leaders and fighters; and 2). The rapid development of the Internet, the global spread of Internet cafes, and the proliferation of personal computers and other means that have the ability to use the Internet (mobile phones). Until the advent of Web 2.0 with its focus on content integration created by the user, social networks and digital videos, bin Laden and "central al-Qaeda" maintained a certain level of control over al-Qaeda's behavior. Abu Musab al-Zaqawi and the al-Qaeda group in Iraq were those who introduced a special online strategy in the period before the end of the Web and the rise of Web 2.0, and thus mark the beginning of the transformation of violent extremist organizations from the movement of a substantial Internet component to an authentically online extremist movement.

Like traditional extremist organizations, online radical groups are communities where perpetrators of violence are in certain subgroups. In other words, terrorist groups and violent extremists come from violent extremist environment, and hence terrorist and generally extremist groups and attacks can also emerge from their online variants. The difference between online extremists from supporters is that in the online extremist's structure, there is a form of social structure responsible for group cohesion. It is not just a set of individuals who represent similar political/cultural attitudes.[4] Violent online jihadist action, as its name suggests, emerged when the jihadi sphere covered a wide range of interconnected creators and consumers, from central al-Qaeda and media weapons to several al-Qaeda franchises, to the globally widespread network of jihad supporters, without linking to any jihadist organization, all contributing to the daily making and renewal of violent jihadist behavior.[5] The changes in the nature of the Internet have encouraged a growing number of supporters of violent extremism to post and edit articles and analyzes, exchange information, opinions, and debate ideas about blogs, websites and forums that they have raised themselves. Proliferation on pages of supporters acted as a free publicity for violent extremist cause. Today new web pages appear, but also disappear frequently, popular chat rooms have rigorous policies for joining, and most pages show technical skills by their creators, including the latest internet tools and "gadgets". Al Qaeda has neither had nor has it provided finance or has any managerial role to these pages. However, they act as an invaluable multiplier of force to foster the cyber-based strategy of the groups.

3.1. Social networks in the function of religious extremist organizations

After the events of September 11 and the campaign to fight the terrorism that followed, a large number of religious extremist groups moved into cyberspace by establishing thousands of websites that promote their messages and activities. Many radical sites were targeted by intelligence and law enforcement agencies, and activists who followed the sites attacked some of them and forced their operatives to search for new online alternatives. There was a redirect to social networks.[6] Social networks differ from traditional and conventional media in many aspects, such as interaction, availability, frequency, usefulness, immediacy and consistency. In contrast to conventional/traditional media, characterized by the one-to-many approach in which only a small number of established institutes disseminated information to an effectively limited audience, social networks allow anyone to publish or access information. New communication technologies, such as incomparably cheap and affordable mobile and web-based networks, have created highly interactive platforms through which individuals or communities share, create, discuss and modify content together. With social networks users of information also act as communicators, significantly increasing the number of information providers in the communications market.

This two-way communication promotes the creation of small, diffuse sets of communicators and groups. Virtual communities using social networks are growing popular all over the world, especially among the younger population. Religious extremist organizations have good reasons to use social networks. First, these channels are far more popular with their auditorium, which allows religious extremist organizations to be part of the trend or tendency. Secondly, social networking channels are easy to use (user-friendly), reliable and free. Finally, social networks allow terrorists to access their

target audience and virtually knock on the door - unlike older models on websites where radical extremists were to wait for visitors to access them.[7]

The most important goals of the terrorists online are propaganda, radicalization and recruitment. They can develop lists of potential recruits or sympathizers through online groups. Just like marketing companies that can see information about members to find potential customers and choose a product that promotes them, terrorist groups can see people's profiles to decide whom to target and how to access it of each individual.

Social networking sites allow terrorists to use a target strategy known as narrowcasting. The narrowcasting is aimed at messages for specific segments by the public, defined by values, preferences, demographic attributes, or subscription. Online, video, nickname, photos and information are set up to match and coincide with the profile of a particular social group. These methods allow terrorists to target especially young people. In the upward trend, terrorist groups and their supporters use predominantly Western online communities, such as Facebook, MySpace and Second Life, as well as their Arab equivalents.

3.1.1. Electronic Jihad

Online platforms used to promote electronic jihad are also used for operational purposes such as instruction, training, data collection, coordination, and psychological warfare. In 2008, in the terrorist attacks in several locations in Mumbai - India, attackers used advanced communications technology, including handheld GPS devices, to plan and launch their attack. Satellite images from Google Earth and mobile phones allow users to locate hostages, especially those from abroad. YouTube videos and posts on Facebook are used to train explosives use, to direct web site followers with instructional materials, promote hacking techniques, and share programs for encryption. These postmodern terrorists are trained in virtual online camps, using the abundant opportunities of new social networks.

3.1.2. Facebook Terrorism

Facebook is the biggest social network. In January 2014, Facebook recorded 1.31 billion users, of which 54 percent are logged on a regular basis, and almost half of the 48 percent are logged every day. Their average age is about 30 years. In the Middle East, Facebook has seen a significant increase membership reached 67 percent in 2010, and in Asia 23 percent.
Special Report of the US Department of Homeland Security, lists several ways to use Facebook by terrorists:
As a way of sharing operational and tactical information, such as bombing instructions, maintenance and use of weapons, etc.;
As a gateway to extremist sites and other online radical content by linking them to facebook pages and discussion forums on Facebook;
As a media outlet for terrorist propaganda and extremist ideological messages;
As a wealth of information for distance surveillance, in order to target.

3.1.3. Twitter Terrorism

Twitter is a free micro-blogging service that allows each account holder to distribute messages called "tweets" that are limited to a length of 140 characters. Twitter messages to users can be open to the public or restricted to other users who have chosen to follow the profile. Twitter can be accessed on its website or via mobile devices. By mid-2013, 554,750,000 Twitter users, they sent around 9,100 messages every second or 58 million messages a day, a very fast growing number. Terrorists mainly use Twitter to communicate with sympathizers. A survey of 76,000 messages on Twitter from Al Qaeda linked al-Nusra Front in Syria revealed that they contain more than 34,000 links, most of which lead to jihadistic content. Twitter messages also included the latest developments from various theater operations and propaganda statements. The official Twitter account of Al Nusra @jbhatalnusra, marked a significant increase in the number of followers. Twitter has become a major environment for active dissemination of links that direct users to digital content hosted on a wide range of other platforms. Twitter can also be used for practical communication. When the US air strikes in Syria appeared unavoidable in August 2013, several jihadist and Hezbollah groups in Syria used real-time

functionality on Twitter to exchange emergency communications, preparing for attacks that they thought were targeted at them. Some experts believe that Twitter could also be used to help terrorists in coordinating current attacks.

An intelligence report issued in 2008 by the 304th US Military Intelligence Battalion, including a chapter titled "The Possibility of Terrorists for Using Twitter", which claims that Twitter can become an effective tool for coordinating terrorists who are preparing to commit militant attacks.

3.1.4. YouTube Terrorism

A gigantic video sharing service has become a significant platform for jihadist groups and supporters, appealing a successful subculture for communicating, spreading propaganda and recruiting new individuals. YouTube's massive global audience allows jihadists to focus on potential conscripts and to the goals of terrorism. As important as the videos themselves, YouTube's usefulness in facilitating social networking among jihadists is as important. The ability to share comments on videos and send private messages to other users, helps jihadists quickly identify themselves, resulting in a dynamic jihadist virtual community. Many YouTube sites have posted terrorist clips, some related to major terrorist events around the world. On April 30, 2010, the Pakistani group Tehreek-e-Taliban created its official site on YouTube. A day later, the terrorist organization posted its first video, claiming responsibility for an attempt to attack the Times Square in 2008. Chechen rebel leader Doku Umarov used a video posted directly on YouTube to take responsibility for the attack on the Moscow Metro on March 29, 2010 by two Chechen women.

The video was posted on the website of the Caucasian Center, a group related to the Chechen jihadist movement. In 2012, dozens of pages on YouTube posted cut-offs from a series of detailed video lessons produced by Al-Din Al-Qasim Brigades, a militant Hamas terrorist wing. Most of the videos were about half an hour long and focused on making bombs and using various weapons. The series was titled "Waa'iddu" (ready), a Hamas slogan extracted from the Qur'an with regard to the preparation of Muslims to fight the enemy.

A study by Maura Conway and Lisa McInerney analyzed online video supporters to promote YouTube jihad with a focus on those posting and commenting on materials promoting the sacrifice originating in Iraq. Most of the beneficiaries who were studied were younger than 35 years and lived outside the Middle East and North Africa, with a large percentage located in the United States. As the survey concludes,..."what is clearly evident is that jihadistic content spreads far beyond traditional jihadist web sites or specifically dedicated forums for sharing videos and social networks - features of Web 2.0 - and in that direction they extend their reach far more than what can be interpreted as their core support base in the regions of the Middle East and North Africa to the population in diaspora, transformed and political supporters".

3.1.5. Terrorism on Instagram and Flickr

Although Instagram and Flickr have a reputation primarily for a trendy but easy way to share photos with friends and foreigners, terrorists have also adopted these photo sharing services. Online jihadists pollute Instagram with radical propaganda with the enchantment of their leaders such as Osama bin Laden and Anwar al-Awlaki, as well as other lesser known al-Qaeda leaders who sacrificed themselves while fighting the West. Other photographic sets include graphic photographs of dead jihadist fighters with the text: "Perfect smile" and "Sins forgotten after the first drop of blood". The captured versions of the erased profiles belonging to Dzhokhar Tsarnaev, one of the two brothers involved in the terrorist attack on the Boston Marathon in April 2013, showed that the young bomber "likes" the photograph of the Chechen militant person Shamil Basayev.

Basayev, who was killed in 2006, was the leader of Chechen radical rebels and is believed to have been the brain for several terrorist attacks in Russia. Flickr created a virtual monument for foreign fighters killed in Syria, followed by the name, place of origin and notes for admiration for their devotion and combat force. Without a doubt, the most important goal of this propaganda is encouraging Muslims abroad to join the fight. In the end, it is easy to get to the heinous photographs of beheading or firing hostages on these pages, such as the example of the "Almurbati1" profile on Instagram, where such content is displayed.

4. Analysis of social networks as an approach to combat terrorism

The greatest threat facing the modern world is the religious extremist groupings embodied in terrorist organizations. Terrorists attack informally using terror at any time and place. There is no more structural battlefield where classical military power is used, but the war against this kind of enemy will be obtained only with the supremacy in knowledge. For that purpose, it is necessary to apply a new type of intelligence in dealing with this type of threat, which is an analysis of social networks.

The basics of the analysis of social networks (also known as network science or network sociology), is that individual nodes (which, depending on the type of network can be people, events, etc.) are related to complex but understandable relationships that form networks.[8] These networks are prevalent in basic order and simple legality. The networks form a structural one the basis of many natural events, organizations and social processes. Terrorist organizations are good for studying using analysis of social networks because they consist of networks of individuals extending to certain countries, continents, with similar economic status and with certain specific ideology. The analysis of social networks can provide important information about the unique characteristics of terrorist organizations, from network recruitment, network evolution and dissemination of radical ideas. The analysis of social networks can be used to understand terrorist networks, inform the relevant counter-terrorism institutions and form the basis for more effective countermeasures of the network war.

The importance of analyzing social networks in the fight against terrorism was recognized even before the September 11th attacks. The book by John Arquilla and David Ronfeldt, named Network and Netwars, which was released before the attacks of The World Trade Center describes the growing networking principles in modern criminal organizations. [9] The premise of the book is that war is no longer a battle between two powers.

A modern war is a network war, a battle with less intensity with terrorists, criminals and extremists with a networked organization. The main limitation of the analysis of social networks, which is applicable to any new and innovative technology, is that the analysis of social networks is only one tool that can be used to understand terrorism and is only one part of the puzzle. Furthermore, the basic assumptions for the analysis of social networks in terms of terrorism may not be completely valid. Despite the non-hierarchical approach, terrorist organizations are not completely organized into a network structure. Also, analyzing social networks needs to try to give an answer to the underlying cause of terrorism.

It is useful to understand how the network evolves and how to destabilize the network, but it is even more important to understand how the network recruits new members and why people want to join extremist organizations and terrorist networks. Social networks are highly variable objects (they change over time and across space). Hence in today's advanced information technology analysis of social networks in the function of anticipating and preventing terrorist attacks, is done through specialized algorithms. They automatically and in real time process the data placed on social networks and with the help of computer technologies make a prediction about possible act of violence by certain extremist groups and organizations, but also the so-called "lonely wolves" acting alone.

5. Conclusion

For a long time, religious extremist organizations have used the Internet to recruit, propagate and encourage data collection and fundraising. They turned to new platforms not only because the anti-terrorism agencies have disrupted their online presence, but because new media offer a huge audience and are easy to use. Terrorist followers, sympathizers, converts and newcomers, through new media find an easier access to access to content produced by terrorists, than what they are facing in researching and registering for access to forums. This trend is combined with the rise in the terror of "lonely wolves": attacks by individual terrorists who are not members of any terrorist organization. Terrorism of lonely wolves is the fastest growing type of terrorism, especially in the West, where all recent attacks by lonely wolves include individuals who have been radicalized, recruited, trained even launched on social networking platforms. The migration of terrorists to emerging online resources is a challenge for anti-terrorism agencies, as well as for an academic who investigates terrorism. The

growing use of social media has allowed radical groups and terrorists to freely distribute ideas in multiple ways, including web pages, blogs, social networks, forums, and video sharing services. The fight against terrorism is behind the manipulative use of new platforms by terrorists. Despite the growing research on the Internet in recent years, effective strategies, tools or tactics to combat terrorism have not yet been provided. The security community needs to adapt strategies to combat terrorism in new arenas, using new types of online warfare, intelligence gathering, and training cyber warriors. The virtual war between terrorists and anti-terrorism agencies is indispensable, dynamic and brutal.

Researchers around the world from the disciplines such as psychology, security, communications and computer science, need to be teamed up to develop tools and techniques for responding to online religious extremist organizations. This challenge multiplies multidisciplinary research topics - intelligence and security informatics, also known as cognitive security, for the study of the development and use of advanced information technologies and systems for national, international and societal security-oriented applications. Recognizing online threats, strategies for combating radicalization recognize the important role that the Internet and social networks play in advancing the violent behavior of extremists. However, due to the importance of the digital environment, the need for developing a separate, more comprehensive strategy for fighting and protecting against online extremist violence has been imposed, and with the help of technology, the resilience of the community will be strengthened.

The new online platforms represent the "increased prolongation of the war by other means" adapted to the famous phrase of von Clausewitz. Cyber space with its numerous and growing online platforms brings new challenges and requires a dramatic turning point in strategic thinking in terms of national security and the fight against terrorism. Strategic scholars should look beyond the current challenges to the future development and increase of social media resources and problems with the anticipation and prevention of terrorists to abuse those tools.

References
[1]   William Gibson, 1984 *Neuromancer*, ACE
[2]   Peter Waldmann, 2005 *The Radical Community: A Comparative Analysis of the Social Background of ETA, IRA and Hezbollah*, Sociologus vol.55
[3]   Nancy K. Baym, 2010 *Personal Connections in the Digital Age*, Cambridge: Polity
[4]   Peter Waldmann, 2008 *The Radical Milieu: The Under-Investigated Relationship between Terrorists and Sympathetic Communities*, vol.2, No 9, Perspectives on Terrorism, Terrorism Research Initiative
[5]   Jarret M. Brachman, 2009 *Global Juhadism: Theory and Practice*, Abingdon Routledge
[6]   Department of Homeland Security, 2010 *Terrorist Use of Social Networking Facebook Case Study*, Public Intelligence
[7]   Gabriel Weimann, 2014 *New Terrorist and New Media*, Washington DC: Commons Lab of the Woodrow Wilson International Center for Scholars
[8]   Albert-Lazlo Barabasi, 2002 *Linked: The New Science of Networks – Perseus*, New York
[9]   John Arquilla and David Ronfeldt, 2001 *Network and Netwars, The Future of Terror, Crime and Militancy*, RAND, Washington DC

Copyright © MILCON 2019