AARMS Vol. 17, No. 3 (2018) 47–62. **10.32565/aarms.2018.3.3**

Social Media and Terrorism[1]

Péter BÁNYÁSZ[2]

Today, terrorism is one of the most significant security risks. The spread of infocommunication technologies (ICT) resulted in new types of challenges. Innovation in ICT tools represents new means that terrorists, law enforcement and armed forces have to face. Some of the actions on different platforms of social media can be included here, which can be considered a challenge for all these organizations trying to adapt to them. Today we cannot talk about cyberterrorists and cyberterrorism, nevertheless this does not mean that terrorists would not use the cyberspace or that this platform would not mean a significant threat. This study aims to examine the correlation between social media and terrorism, including psychological operations and intelligence to several other areas.

Keywords: *terrorism, social media, Islamic State, PSYOPS, OSINT, social engineering*

Introduction

Cyber threats are categorized into four groups in the literature. These are: [1]

- cybercrime;
- cyberterrorism and hacktivism;
- cyber espionage;
- cyber warfare.

The purpose of cybercrime is to gain material benefit using IT systems, its targets can be both business and political actors. [2] Although hacktivism and cyber terrorism are conceptually two different phenomena, common points can be identified. In both cases, we can talk about decentralized, small groups, whose purpose is to represent the ideology they advocate before a larger media attention. Hacktivists basically consider the free access to information one of the most important values, and they carry out their attacks for this purpose. The concept of cyberterrorism was first used in the mid-1980s but there is still no generally accepted definition for it. [3] According to Keith Lourdeau *"Cyberterrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda."* [4] In case of hacktivism, a paradigm shift can also be seen; instead

[1] The work was created in commission of the National University of Public Service under the priority project PACSDOP-2.1.2-CCHOP-entitled "Public Service Development Establishing Good Governance" in the Concha Győző Doctoral Program.

[2] Ph.D. candidate, Assistant Lecturer, National University of Public Service, E-Governance Institute; e-mail: banyasz.peter@uni-nke.hu

of amateurs, professionals well supported by politics use this tool, who many times attack with a military purpose, such as the hacktivists of the Islamic State or the Syrian Electronic Army. [5]

However, we can tell that, fortunately, there are no cyber terrorists at the moment, although there are terrorists who use the Internet. Cyber espionage means the intelligence activities of states or market players are carried out on IT tools, and cyber warfare occurs in case of conflicts between states, in which conventional warfare is supported (or triggered) in order to render the information systems of the opponent state completely inoperative.

Terrorism can also be identified as one of the most significant security risks because it unites the toolkit of cybercrime and cyber espionage and aims to create such a capability with which it is empowered to carry out cyber warfare related actions. However, social media was initially a means of communication, but its spread and ever-expanding functions provide many opportunities for both terrorists and criminals.

The Emergence of Cyberterrorism in the Scientific Community

I've conducted a keyword analysis using the Scopus database. Scopus, founded in 2004, is the largest abstract and citation database of peer-reviewed literature, which enables the analysis of scientific journals, books and conference proceedings. I've built my database based on the keyword "cyberterrorism" using Scopus. The search concerned every scientific statement that included the search term "cyberterrorism" in its title, abstract or keywords. The database, similarly to Google search, only interprets the connection between words based on several keywords if they are in quotation marks, otherwise every result will be displayed that include the terms "cyber" or "terrorism". The search was conducted with this restriction. I've examined the result list according to scientific domain distribution.

The reason for the keyword analysis is the fact that the more frequently a certain keyword occurs the more relevant it can be viewed. I've conducted a trend analysis based on the occurrence of relevant keywords in order to examine whether a pattern could be determined for the proliferation of single keywords.

Further, I've conducted an international examination by limiting the scope to Hungary in order to find out how researches related to Hungarian cyber security are fitting in global trends.

Up until 2018, to August 2018 included, Scopus found 188 results on the search term "cyberterrorism". Figure 1 shows the scientific domain distribution of statements.

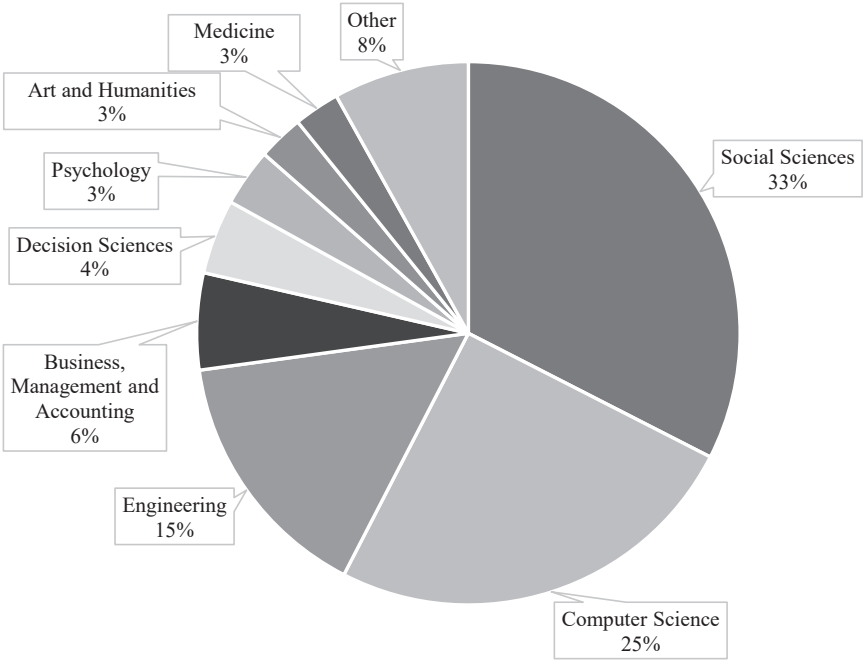

Figure 1. *Distribution of the search terms cyberterrorism globally per scientific domains according to Scopus.* [Based on Scopus; edited by the author.]

As shown in the figure, publications of technical nature are dominating researches related to cyberterrorism, 32.2% of all publications can be subject to Social Sciences and 24.8% to the scientific domain of Computer Science.

Table 1 shows the distribution of each publication according to country based on the top 8 countries.

Table 1. *Top 8 distribution amongst countries on the search term cyberterrorism.* [Based on Scopus; edited by the author.]

Country	Documents
United States	68
United Kingdom	25
Ireland	7
Australia	6
Netherlands	6
Germany	5
Israel	5
South Korea	5

Scopus database only stores 3 scientific statements after narrowing down the scope to Hungary. 100% of all publications can be subject to Social Sciences.

Figure 2 contains the yearly distribution of each publication. It is apparent that the first result for the search term cyberterrorism can be dated back to 1997.

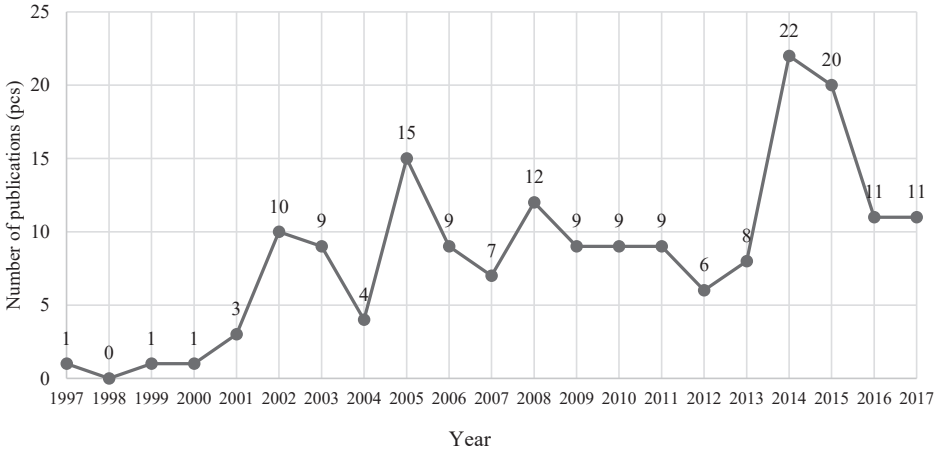

Figure 2. *Yearly distribution of the number of publications globally based on the search term cyberterrorism.* [Based on Scopus; edited by the author.]

The trend of the number of Hungarian publications is represented in Table 2.

Table 2. *Yearly distribution of the number of publications in Hungary based on the search term cyberterrorism*
[Based on Scopus; edited by the author.]

Year	Documents
2009	2
2006	1

The publications include overall 459 keywords, which needed to be narrowed down in order the manage them in a consistent manner. This was justified by the use of the singular and plural form of each keyword, by their different spelling,[3] and typos. In table 3 I've displayed those search terms where the result rate was over 3.

Table 3. *Occurrence of keywords in scientific statements for results on the search term cyberterrorism.* [Based on Scopus; edited by the author.]

Keyword	Occurrence
cyberterrorism	59
terrorism	25
internet	20
cybercrime	12

[3] For example cyber terrorism, cyberterrorism, Cyber terrorism, Cyber Terrorism, Cyberterrorism.

Keyword	Occurrence
cybersecurity	11
security	7
cyberspace	7
propaganda	5
postmodernism	5
networks	5
hacking	4
information security	4
cyberwar	4
counterterrorism	4
cyberattack	4
attack	3
critical infrastructure	3
cyber threat	3
semiotics	3

I've built another database based on the keyword "cyberterrorism" and "social media" using Scopus and found 3 results. The publications include overall 9 keywords. In table 4 I've displayed those search terms.

Table 4. *Occurrence of keywords in scientific statements for results on the search term cyberterrorism and social media.* [Based on Scopus; edited by the author.]

Keyword	Occurrence
cyberterrorism	2
affiliation	1
authur pendragon	1
cyber threat	1
mimetic virus	1
rumor mongering	1
social attachment model	1
social media	1

Social Media and Cyberterrorism

Numerous attempts have been made to define social media, the vast majority of which are related to the field of marketing, which at the same time bears the impression that it operates primarily with marketing-related concepts. The online Oxford Dictionary [6] describes social media as a set of web pages and applications that allow users to create and share content on social networks. This concept originates from Andreas Kaplan and Michael Haenlein, according to whom, social media is a *"set of internet applications that builds upon the ideological and technological basis of Web 2.0, which promotes the creation and transformation of user-generated content."* [7: 61]

Accepting the concept of Kaplan and Haenlein, but complementing the definition, social media is considered to be a set of web pages and applications in which the service provides

only the main frameworks, but the content is generated by the users. It follows that social media consists of primarily the interactions of users and, including the share or supplement of other users' content which can mean the production of totally new content. Theoretically, this content may change or expand by the effect of new information. Social networking sites have become a part of our daily lives: the inevitable parts of homes, workplaces, schools and leisure. Figure 3 shows the most popular social web sites.

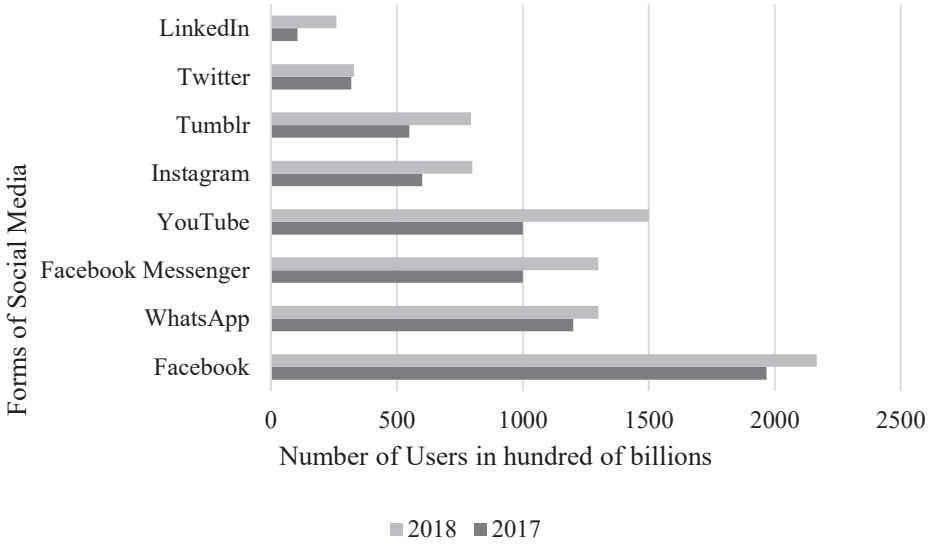

Figure 3. *Social media sites by visits globally 2017–2018.* [8] [Edited by the author.]

It is no exaggeration to say that social networking sites have been used by Islamic State terrorist groups in a paradigm shift way. In the followings, the areas of application how terrorists use or might use social media sites will be examined through the example of the Islamic State. Terrorists can use these websites for the followings:

- obtaining information;
- social engineering;
- contacting;
- propaganda;
- recruiting new members;
- receiving supporters;
- committing psychological operations;
- cyber-attacks.

Although the importance of the Islamic State has diminished considerably by today, the procedures and technics used by them, in my view, can be considered the examples of how future terrorist groups would use social media sites.

Obtaining Information and the Social Media

When designing a terror attack, selecting the target, spot, date, tools and methods mean the starting points. Collecting the right information is essential for which the *open-source intelligence* (OSINT) is an important tool. Following the concept of Lévay Gábor *"OSINT means the research, collection, selection, analysis-evaluation and use of not-classified data which are legally and publicly available (for everybody) based on professional aspects besides the military intelligence."* [9:6] Taking into account that open-source intelligence can be carried out by anybody, and scouts and operators of terrorist groups can obtain a huge amount of information from the internet and social media sites, the right data and information sensitivity have become crucial. [10] However, the OSINT is a necessary but not a sufficient condition of intelligence. In case the target of a terrorist group is a traffic subsystem, even though they have access to the Google Earth, satellite images of the area taken by Street View, or 3D panoramic photos, the going-over of the area cannot be neglected. Social media is the golden mine of the open-source intelligence. One of the main reasons is that the average users of these sites do not have sufficiently high data and information awareness so they share many moments of their lives. The longer and the more social media sites are used, the more detailed profile can be built up about the user—in case the visibility is not limited.

The activity itself can be really long if the operator is not familiar with the methods, but there are websites that accelerate it.[4] We need the ID Number of the target person which can be obtained by websites generating ID Numbers.[5] For this, the link of the Facebook profile of the target person should be copied to the website, and the ID number will appear in a few seconds. Then, the ID number should be pasted to the right cell to get the required information. Such information can be for example the places we have visited, what pages we have liked, the groups we are members of, images, posts liked or commented by us, events we have registered, colleagues, friends, etc. It is important to note that the website will display only the open-source information. This means it will not display anything which are not publicly shared, nor the personal messages. The majority of these information can be blocked also, but in case we comment under the post of a friend who has not limited the visibility of the post, then our comment will be displayed as well.

On the other hand, there are information which cannot be blocked, page likes, the list of applications which we have used, membership of groups, etc. In case we do not know our target person, fortunately (?) we can still browse[6] based on several variants if we know some information about this person, e.g. address, age, what he/she likes, etc. This way, we can select the targets based on the given features, who can be taken under further examination later. Of course, users will be displayed only if they have let the visibility open on their pages.

In my opinion, the applications developed for smart devices mean a kind of grey zone of open-source intelligence, that require certain permissions in return for the use. Every application, being free or paid, requires different permissions. These can be varied, but normally require only essential permissions for the application's function. In case of

[4] A good example is the webpage of www.uk-osint.net/facebppl or the https://inteltechniques.com/OSINT/facebook.html

[5] See also http://lookup-id.com/

[6] See also www.peoplefindthor.dk/

a flashlight application, it is adequate to access to the flash, likewise in case of a dictaphone application to the microphone control and to device's storage and modify it, in case of a messenger to our messages, or a photo application should have access to the camera, etc. The problem comes when the users are not careful enough when installing an application, and they do not read what permissions they give for the application. The application then may also get such permissions which are not necessary for their function. The information gathered this way, which can consist of everything stored on our mobile devices, are later sold for marketing purposes, but they can become the tool of target monitoring because a camera or microphone control, or the access to the user's messages let the developers of the application monitor and intercept the user at any time even real time. Not to mention, that some applications store medical data about us,[7] the security of which is extremely important. We can add a list of things we are allergic of, which can be important in case of emergency. This is really important and useful, but the problem is that if the security of our devices is not appropriate, the applications can obtain all stored information. This can be circumvented by offering food containing the ingredients the potential victim is allergic of, and being consumed these ingredients can cause harm.

It is a grey zone because even though the user gives several permissions for the applications in return for the use, this can relate to information which cannot be classified as open information at any time. The geo-positioning, the list of our friends, our profile photo can be open information in case the user treats them as open information, but the question of whether our friends treat their own networks as open information arises. Besides the already mentioned examples, we can permit the access to our messages, which, in my opinion, cannot be classified as open information at any time.

Social Engineering and Social Media

Collecting information does not play a role only in designing, but it is essential also in social engineering. The social engineering is a form of attack when the attacker exploits human factors[8] to gain access to protected information or systems by deceit or extortion. [11] According to Kevin D. Mitnick[9] *"The social engineering deceives people, manipulates or persuades them that the social engineer is really the one who he is said to be, by manipulation and persuasion. As a result, the social engineer—by the use of technology or without it—is able to exploit people to gather information."* [12: 1]

The social engineering is usually categorized by human [13] or IT [14] based attacks, whether an IT tool is used while carrying out the attack. These types of attacks can be effective

[7] What is more, with the iOS Health application we can save medical certificates on our cell phones and share them with other devices.

[8] Naivety, gullibility, assistance, curiosity, lack of security awareness, inattention, sexuality, etc.

[9] According to Kevin Mitnick, one of the most famous hackers these days, who has never considered himself a very prominent hacker, he could succeed mainly by social engineering. After being arrested, he broke up with illegal penetrations, founded a security firm and is currently working as an ethical hacker.

even if the target system has been strengthened by physical and logical security.[10] The danger of this was proven by the experiment of two security experts by connecting a fictitious young, female user with unreal Facebook and LinkedIn profiles to employees of an unidentified US government agency working in the field of cyber security. [15] The result is astonishing: during networking activities the experts have infected the computers of the employees by an e-postcard, so they got access to their confidential data. The senior officer responsible for the agency's IT security was among the victims, as well. It is not hard to understand that this way terrorists can easily enter platforms which are strictly protected (for example, by extorting a member of a security staff).

Contact and Social Media

Due to the particularities of terrorism, the operation of the groups must be characterized by a high level of conspiracy. Social media sites and applications mean new sets of tools of conspirative contacting. The methods of this can be different depending on whether the contact is real time or not. In the latter case, we can talk about placing a message in the form of a blog post, supported by lyrics, or a video uploaded, which let decode the message only for the insiders. The tools of real-time contact are the different chat rooms and the not public chat rooms of online social games.[11] Based on the information coming to light by Edward Snowden, it may be assumed that terrorists use these methods regularly, as the National Security Agency (NSA) maintains a separate department to coordinate agents infiltrating to online games.

Propaganda and Social Media

The terrorist groups recognized the relevance of their recordings about the terror attacks for propaganda purposes relatively early during the Chechen wars. Ibn al-Hatták Saudi guerrilla leader is considered the first Jihadist, who recorded his outrage for this purpose. Nowadays, in the age of social media, the number of tools used by terrorists for scaremongering, recruiting new members, convincing supporters, propaganda, intelligence and cyber-attacks has been excessively increased.

The Islamic State has published regularly their actions in the social media: crucifixions, mass executions, decapitations, etc. When designing terror attacks and selecting the target, it is of utmost importance that the attack implemented provides the utmost publicity. [16] Propaganda is one of the most important elements of organizational existence.

One of the aims of a terror attack is to draw attention to the principles of the terrorist group, for example the critique of the consumerist society, or the fight against repression, etc. Because of this, when selecting the target, newsworthiness gets priority. Due to this,

[10] Physical security means the protection against threats in the physical space, including the protection from natural disasters, mechanical protection, electronic control system, security personnel, identification systems, surveillance systems, power supply, air conditioning and fire protection. Logical security means the protection of IT systems provided by IT tools and procedures (software, protocols).

[11] For example, World of Warcraft, Second Life.

propaganda has different purposes: increasing the visibility of the terrorist group by the news about their attacks, representing their declared purposes, scaremongering in the groups defined as enemies, recruiting new members and supporters.

Psychological operations are one of the most important tools of propaganda. Psychological operations, based on the dissertation of Pix Gábor written in the topic, are the actions in which the opposing parties use conscious psychological influences to achieve their goals. [17]

The first station of the Islamic State's propaganda was the choice of the name; from their establishment in 2003 to the declaration of the Caliphate in 2014.[12]

The Islamic State carried out its propaganda at master's level. Contrary to the Al-Kaida's poor quality propaganda videos, the Islamic State spread their videos on numerous platforms of the social media in HD quality, in English with Arabic subtitle with hashtags.

József Margitics summarizes these platforms in his study. [18] Based on the list of the author, the followings are included:

- Jihad Media Platform website, where the registered users can share news and comments. In 2015 the number of registered members exceeded 3,000, who written more than 400 thousand comments. News could be found by regional breakdown, fresh news—in multiple languages, including English, French and German. Topics about the Coran, propaganda photos and videos, but also posts about family or health topics have been published.
- Islamic State Archives website, where reports, photos, videos including the messages of soldiers have been shared for recruitment and propaganda.
- There have been several pages and groups on Facebook, including the fresh news of the Islamic State, Mujahed's news, Abu-Bakr Baghdadi etc. Groups: "United Islamic Cyber Force" network, Umma Jihad on top, and the media of the Islamic State, etc.
- In the first half of 2017, nearly 300 thousand terrorist propaganda profiles have been deleted from Twitter. The deletion of accounts has become intensive since August 2014, that can be attributed to the decapitation of the American journalist, James Foley.[13]
- There have been numerous YouTube channels as well, showing the training, messages of detainees and moments of everyday life. In addition to this, to find the common voice with the youth to show the "cool" side of the terrorist group, they integrated terror actions, flags and clothes into videos based on the GTA V game.
- Dabiq and Rumiyah online newspapers contain news, tactics and also propaganda.
- Mobile applications have been used not only for contacting, such as the Telegram Messenger, but also for propaganda. After executing James Foley, when their profiles

---

[12] In 2003 it was known as Iraqi Al-Qaida, in 2011, when the civil war broke out in neighboring Syria, the Iraqi and Levantei Al-Qaeda names appeared there, expressing the fact that Eastern Syria and northern Iraq were one. During the civil war in Syria, the ideological difference with Al-Qaeda, which essentially regards the struggle against the West as an organizing element, has been demonstrated, and the Iraqi and Levantei Al-Qaeda Islamic Caliphs are working on it. Of course, the ideals of Al-Qaida appeared in the early 2000s as the idea of the global Caliphate, which was intended to be the outcome of a 20-year plan, but it was represented by the Islamic State in the early 2010s. This ideological discrepancy led to the suspension of violence, and in the end, in 2013, the Islamic State of Iraq and Levante (ISIS) was renamed to the known name change in 2014.

[13] Shortly after Foley was executed, a video on the murder of another abducted US journalist Steven Sotloff was accidentally released to the Internet, which was, however, not part of the IS's propaganda, because it was published beforehand for which the Islamic State was formally apologized to his followers.

and channels have been started being deleted, the Islamic State developed an application with the title *Dawn of Glad.* The application was available for downloading from Google Play for a long time. In exchange for downloading, the users gave permission for the application to share news in their name on their social websites. This way the Islamic State became ineradicable from social media.

- Several blogs, including the Islamic Caliphate and Islamic State has shared propaganda messages and news with a similar content as the above-mentioned examples.

The intensive presence of the Islamic State in the social media reached a lot of Western youth who, giving up their lifestyles, joined the organization.

According to some assumptions, Ahmad Abousamra, a Syrian–American IT expert, who had formerly worked for telecommunication companies, is responsible for the professional presence of the Islamic State in the social media. [19] Contrary to the previous poor quality videos shared on VHS and not too modern communication strategy, the IS caught the youth's attention by high quality, professionally designed videos, and hash tagged[14] Twitter campaigns. It is no accident then when recruiting new members, the Islamic State emphasizes the points which are easily understandable for youth and determining the organization as a youthful, cool group. The organization stresses particularly on children, as it became apparent from the report of Medyan Dairieh prepared for Vice News. [20]

An important tool for psychological operations is the propagation of fake news, the success of which can be best described by the "post truth" phenomena. The post truth concept describes a situation when public opinion is not based on facts but influenced by emotions and convictions.

Cyber-Attacks and Social Media – The Future?

In the introductory section of this paper, I stated that even though currently terrorist groups are not able to carry out attacks related to cyber warfare, they intend to develop their capacities in this direction. A complex cyber-attack against critical infrastructure requires a high level of technical knowledge, but on the Darknet[15] cyber criminals offer different services which can be used for serious cyber-attacks. The Internet Organised Crime Threat Assessment published in 2016 by the Europol defined the concentration of the cyberspace and terrorism as one of the main focus. [21]

The role of social media can be identified indirectly in the cyber warfare in the infection of IT tools by malicious software, which is called computer-networking operations. These operations serve two purposes. On the one hand, they are used for network detection, and gathering information, on the other hand, modifying, interfering, destroying the gathered information or achieving dysfunction in networks. [22]

---

[14] Hashtag was first introduced and disseminated to other platforms by Twitter. It means a simple tag system that allows to filter and categorize different contents and serves as an easy way to skip between different contents within a given topic. Hashtags can be generated by the # symbol.

[15] Darknet means the webpages on the Deepweb platform where supported by high level encryption, illegal assets and services can be bought, including weapons, narcotics, assassination, sexual services.

Malwares seem to be ineradicable from social media. They appear as campaigns and often cause massive infection. However, they can be relatively easily filtered, the features indicating the links and videos infected by malware codes; they appear regularly, often infecting the same victims as before. The features of the malwares expanded on social media platforms such as Facebook are the followings:

- we get message from our friend in a foreign language that he does not speak;
- link or video promising erotic content about a celebrity or about ourselves;
- our friends tag us in a bulk at a shared content;
- abbreviated link promising the above-mentioned contents or any other sensation;[16]
- content promising huge discounts (e.g. branded sunglasses for some dollars, etc.).

The computer infected this way can be used for a lot of things depending on the purpose of the developer of the malware. These can be the followings:

- our device can become a member of a botnet network, and our resources can be used by the attackers to reach their aims, e.g. mining crypto currency, sending spams or DoS attacks;
- ransomwares can be placed on our device that encrypt our files;
- can give access permissions to our system;
- spywares can be placed on our devices.

The Possibilities of Defence

In the previous section of the paper we could see that terrorists use a wide range of tools to achieve their aims and the past examples confirm that whenever they get the chance, and their capacities make them able, they will carry out such attacks that have not occurred so far (e.g. a cyber-attack against an essential constituent). In early 2013, presumably Chinese hackers broke into the system of the US Army Corps of Engineers which led them gather information about 79 thousand dams. The dams are not only the important elements of energy producing but entail high risks because by obtaining control over them, in case of inundating the nearby areas they jeopardise human lives. [23] We should not have illusions then, we must be prepared for this kind of attacks as well, because their occurrence is only a matter of time.

In the followings, I introduce the possibilities that can be used, that have to be used by the counter-terrorism organizations for prevention and remediation. These statements intend to reflect the results of the examination of the previous section. Accordingly, operations are necessary to be performed mainly in the following areas:

- counterpropaganda;
- psychological operations;
- mapping networks;
- intelligence;
- communication monitoring;

[16] In the case of abbreviated URL, it does not always mean risk, but it should be suspicious when it is sent by an acquaintance who does not know how to make URL abbreviation.

- integration;
- monitoring, disqualifying, recruiting managers;
- trend analysis;
- education;
- recruiting supporters and experts;
- inducing political decision making.

As we could see, terrorists place particular emphasis on "winning hearts", so one of the main tasks is the organization of counterpropaganda. This is not only relevant for the given state, but it is essential in the operations of Civil-Military Co-operation (CIMIC). As the IS finds the common voice with the youth, the counter-campaigns must also use those platforms where the targets of terrorist recruiting are present. Not only the Western European and American youth but also the population of the mission territories have to be considered as priority target groups in the counterpropaganda since it cannot only play a role in justifying the presence, but they are the elements of legitimacy of actions of terrorist groups in the fight against foreign invaders. One of the main points of the CIMIC is that the local population should not consider their presence an invasion, and should not perceive those who serve there as enemies. The notorious Abu Ghraib jail and the related violations have increased the opposition of the local population against the mission units. The strengthening of the Islamic State is explained by the dissatisfaction and mistrust with the corrupt Iraqi political and military leadership, which is compounded by the close relationship with the United States. It is therefore important to carry out counterpropaganda on the social media sites.

The network dimension of social media comes from its conceptual definition. Therefore, the methodology of network analysis provides an excellent tool to map the relations and networks on social media sites.

The role of social media in intelligence cannot be approached only from the aspect of OSINT. From the information coming to light by Edward Snowden, the relevance of Signals Intelligence (SIGINT) can be outlined for anybody, one part of this is the monitoring and analysis of the data generated on social media sites. The introduction of the Snowden case is not included in this article because its complex analysis would take multiple pages. Here, we must mention the relevance of the fact that the national security services can access the whole communication of any user. The monitoring may be mass or individual.

As terrorists use the different social media sites, chat rooms, online games, the presence of authorities is also necessary which in case of success results in the infiltration into the organization itself. By the information gathered applying SIGINT operations, possibilities to compromise the target people arise, with which or the recruitment, or in case of denying cooperation, disqualification can be achieved. From the Snowden documents, we got to know that the NSA has monitored the porno watching habits of several Muslim leaders. By using these devices, we can gather a lot of compromising information, as I have verified this using smart phones.

Taking into account the take-up of social media sites, the systematic analysis of different blogs and social networks, etc. provides the possibility for real-time and automated analysis and the preparation of prognosis and trend analysis of communication and content sharing on a national, as well as international level. The programs used by national security services

can synthesize and visualize huge amount of data. Besides this, these programs are developed constantly, which drives towards the development of artificial intelligence. For example, the American Secret Service has published an open call for the development of an application that is able to detect sarcasm in the media. [24] Considering the extent an average user can detect it, if the algorithm approaches this, in my opinion, we can talk about success.

Social media gives the chance for the users to develop their data and information sensitivity. We need to create campaigns not only to develop their awareness, but also to reduce the spread of different malicious software, which may cause cyber-attacks. Taking a look at the experiment of Aamir Lakhani and Joseph Muniz in the previous section, we could see what kind of dangers the inappropriate data and information protection may contain, so the education of the right internet use is crucial for the staff working in the defence sphere.

All the above-mentioned processes have followed the principle of "action-reaction". It is also relevant for counter-terrorism how terrorists intend to recruit supporters by propaganda. Counter-terrorism actions are not performed by the public opinion because it is the main task of counterpropaganda. The significance of cybersecurity does not even need to be emphasized, but reaching the appropriate capacities is not possible without experts. One tool of this can be the involvement of the domestic hacker community.

In addition to the experts dealing with counter-terrorism, politicians play an important role, as well. One of most significant steps has been carried out by Germany in the fight against fake news. In the summer of 2017, a new legislation was adopted to punish up to 50 million EUR those social media sites which do not remove contents applicable for incitement to hatred within 24 hours.[17] The legislation entered into force on 1st January 2018, and it must be enforced in case of every social media site having at least 2 million German users. If the user enters the site from a German IP address, he/she has to see a platform on which they can register the post applicable for incitement to hatred or being against the German constitution or being a criminal offense. Altogether twenty German laws allow registering these posts, including the legislation on the prohibition of arbitrary symbols, and the attempt to subvert the constitutional order.

In order for the social media sites to comply with the statutory provision, the number of moderators has been enlarged who must decide whether the registered content is really infringing and, if so, should be deleted. A number of German political parties and lawmakers have raised their voices against the law.

The most significant argument is the privatization of the judiciary, as deciding that something is unlawful is normally the task of courts. This cannot be taken over by companies. Related to this, this regulation imposes an extremely short deadline for making the decision, so there is no guarantee that a huge amount of content will be deleted automatically without reading the content in detail, and this can lead to a censorship. Besides Germany, Great Britain is considering a similar regulation, and the French President, Emmanuel Macron has also announced that the French media regulation will be reviewed to fight against fake news spread on social media sites.

In January of 2018, Mark Zuckerberg announced that they would modify Facebook in a spirit of fighting against fake news. The modifications would highlight the posts of our friends and overshadow news portals. This step has attracted a lot of criticism, because this

[17] In case of unspecified content within a week.

way not only the portals of fake news would be reduced radically but also the sites which do not pay for the display.

It is not a question, that we must take action against fake news and contents of incitement to hatred. These are not only political contents but other harmful contents, such as fake news against vaccination, and contents about harassment. But the way to regulate effectively these national social media sites is a very complex and difficult question; no appropriate answer to them has been born so far. If the anonymity decreases, which was a basic principle of the internet in the beginning, the governments and social media sites would know much more about the users and this would infringe the freedom of expression. This would not only increase the censorship of governments and companies but self-censorship, as well. Furthermore, it should not be neglected that even if a social media site is related to one country, it can have global impact; so for example the American practices may intervene in the life of other sovereign states. Referring back to the German regulation, the social media sites would have limited incentives in the anonymity of their users, and this would lead to the internet's high level of regulation, foreseeing public control of a State.

Summary

In my study, I attempted to present the role of social media in counter-terrorism. For this purpose, I examined the possibilities terrorists can use to achieve their aims, and the possible reactions. In view of the limited space, the paper described only the theoretical frameworks, the listed points would require further researches. I believe that if once we open Pandora's box we cannot close it anymore. It is especially true in terms of terrorism as it can be seen in case of the Islamic State. New methods and new procedures are created constantly and even if we learn coping with them, another appears. We can successfully react to these only if we do not refuse the use of these new technologies and tools and we constantly renew them.

References

[1] KRASZNAY Cs.: A polgárok védelme egy kiberkonfliktusban. *Hadmérnök*, VII 4 (2012), 142–151. http://hadmernok.hu/2012_4_krasznay.pdf (Downloaded: 18.03.2018)

[2] MOSKOWITZ, S. L.: The Global Cybercrime Industry. In. MOSKOWITZ, S. L.: *Cybercrime and Business – Strategies for Global Corporate Security.* Oxford: Elsevier LTD, 2017. 3–22.

[3] LUIIJF, E.: Definitions of Cyber Terrorism. In. Akhgar et. al. (ed.): *Cyber Crime and Cyber Terrorism Investigator's Handbook.* Oxford: Elsevier LTD 2014. 11–17.

[4] fbi.com: *Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security February 24, 2004*. www.fbi.gov/congress/congress04/lourdeau022404.htm (Downloaded: 18.03.2018)

[5] CALDWELL, T.: Hacktivism goes hardcore. *Network Security*, 5 (2015), 12–17.

[6] oxforddictionaries.com: *Definition of social media in English.* www.oxforddictionaries.com/definition/english/social-media (Downloaded: 23.13.2018)

[7] KAPLAN, A., HAENLEIN, M.: Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, 53 1 (2010), 59–68. DOI: https://doi.org/10.1016/j.bushor.2009.09.003

[8] *Statista*, www.statista.com

[9] LÉVAY G.: *OSINT (Open Source Intelligence) – Nyílt információs hírszerzés.* (egyetemi jegyzet) Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2006.

[10] STEELE, R. D.*: Searching for Bin Laden: The Use of Intelligence in the War on Terror or How NOT to Spend the Taxpayers' Treasure.* (The Smart Nation Act: Public Intelligence in the Public Interest, Foreword by Congressman Rob Simmons (R–CT–02) Sponsor, The Smart Nation Act.) Oakton: OSS International Press, 2006.

[11] DEÁK, V.: Biztonságtudatosság az információs környezetben. *Szakmai Szemle*, 3 (2017), 59–77.

[12] MITNICK, K. D.: *A legendás hacker. A megtévesztés művészete.* Budapest: Perfact-Pro, 2003.

[13] DEÁK V.: A social engineering humán alapú támadási technikái. *Biztonságpolitika*, 2017. április 10. http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-social-engineer-ing-human-alapu-tamadasi-technikai (Downloaded: 21.03.2018)

[14] DEÁK V.: A számítógép alapú social engineer támadási technikák. *Biztonságpolitika*, 2017. április 28. http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-szamitogep-alapu-social-engineering-tamadasi-technikai (Downloaded: 21.03.2018)

[15] LAKHANI, A., MUNIZ, J.: Social Media Deception. In. *RSAConference Europe.* Amsterdam, October 29–31. 2013. http://itcafe.hu/dl/cnt/2013-11/102992/hum-w01-social-media-deception.pdf (Downloaded: 12.08.2014)

[16] HORVÁTH L. A.: *A terrorizmus csapdájában.* Budapest: Zrínyi Kiadó, 2014.

[17] PIX G.: *A lélektani műveletek jellemzőinek vizsgálata.* (PhD-értekezés), Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2005.

[18] MARGITICS J.: *Az ISIS által használt internetes propaganda eszközök áttekintése.* Budapest: Nemzetbiztonsági Szakkollégium, 2017.

[19] McPHEE, M., ROSS, B.: Official: *American May Be Key in ISIS Social Media Blitz.* http://abcnews.go.com/blogs/headlines/2014/09/official-american-may-be-key-in-isis-social-media-blitz/ (Downloaded: 03.09.2014)

[20] DAIRIEH, M.: *The Islamic State (Part 2).* https://news.vice.com/video/the-islamic-state-part-2 (Downloaded: 17.08.2014)

[21] Europol: *The Internet Organised Crime Threat Assessment 2016.* Hague: Europol, 2017. www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assess-ment-iocta-2016 (Downloaded: 02.04.2018)

[22] ANDRESS, J., WINTERFELD, S.: *Cyber Warfare (Second Edition). Techniques, Tactics and Tools for Security Practitioners.* Waltham: Elsevier Inc., 2014.

[23] GERTZ, B.: *The Cyber-Dam Breaks.* http://freebeacon.com/the-cyber-dam-breaks/ (Downloaded: 11.09.2014)

[24] ZEZIMA, K.: *The Secret Service wants software that detects social media sarcasm. Yeah, sure it will work.* www.washingtonpost.com/blogs/the-fix/wp/2014/06/03/the-secret-service-wants-software-that-detects-social-media-sarcasm-yeah-sure-it-will-work/ (Downloaded: 21.09.2014)