WAYS OF CYBERTERRORISM

Commander Professor Sorin TOPOR, PhD*

Cyberattacks are now becoming more and more complex, more frequent and with increasingly destructive effects. Regardless of the type or value of an organization, it affects information of public and private infrastructures. Moreover, the target may be the private information of those who hold, even temporarily, various public or official positions in a state. In other words, cyberattacks can be directed towards the information profile of a target by affecting data about identity, about finance, by changing information from personal conversations and other private life activities etc.

In this context, terrorism aims to perform actions with clear goals, only once or in series, having as motivation the resistance to political, economic or social changes and producing global information effects. It is well known that the development of terrorism is favored by the development of information technology. Through these, terrorist organizations seek to enhance the perception of terror, by capturing the attention of the global media and by transmitting apocalyptic messages. On the other hand, the anti-terrorist structures are trying to stop or at least hold under certain control these directions of evolution.

The purpose of this article is to determine the content of the concept of cyber terrorism, starting from the analysis of the main factors of public insecurity and social disorder that facilitate the development of modern forms of terrorism. In order to do so, we will try to underline the essential aspects that are relevant for understanding the forms it takes and the ways it works.

Keywords: terrorism; cyber terrorism; cyber spying; cyber frauds; e-propaganda; e-training; radicalization.

At present, within human society, information flows very rapidly through the modern IT&C capabilities. Thus, the mass-media strengthens its function as a basic tool for analyzing, transmitting, shaping opinions, setting or correcting working agendas etc., all of which have as their primary objective the "trade of information". Therefore, the information sold must be beautifully presented in suggestive images, if it is a material situation and/or with charismatic attributes if they stem from socio-human life situations. For this, real science has emerged, such as: neuromarketing, image counseling, clothing consultancy etc.

We could say that all of these have the main purpose of capturing the attention of a target audience, whether trained or not, educated or not. Thus, we notice that the traditional methods of communication can no longer be the only ones used in order to capture the attention of a target population segment. For a media action to be successful, the audience needs to be seduced with information. Moreover, in order to reach the feelings of the people in the respective audience, modern information techniques and technologies are needed to optimize the abilities to communicate at global level. We also refer to the easy access to Internet services, news services provided by various TV and radio channels and print media, other services and communication technologies such satellite communication, mobile phones etc.

As terrorist organizations promote extreme violence, they also have their audience. This audience is seduced by stimulating the perception of having a high level of „psychological power" over other persons. Only thus could we explain why this type of audience listens to and supports the message sent by the leaders of the terrorist organizations. The most eloquent examples come from the current conflict areas from Afghanistan, Middle East, Africa etc., areas where the armed reaction is encouraged by stimulating people's perception that the US led the warfare against Islam; or in the Palestinian-Israeli area where the idea promoted is that of discretionary application

*"Carol I" National Defence University
e-mail: *sorin.topor@yahoo.com*

of citizenship or visa-granting policies on the highly complex migration situation from the ISIS/ Daesh-controlled areas; or in other areas of "social resistance" where there are anarchist groups and vigilantes who militate for so-called "defence of human rights through violence" as a form of social reaction to abuses of intelligence services and other governmental institutions (ex: yellow jackets movement, in France, in 2018).

Under these circumstances, we may say that the main target of contemporary terrorism is to obtain or maintain public insecurity and social disorder within the state. If within this information society – attribute increasingly used for characterizing the current stage of social evolution – information has become more significant than the other social dimensions, terrorist organizations also undergo changes being compelled to adjust communication methods to the demands of information consumers. Thus, keeping in mind these traditional terrorism patterns, we may state that cyber terrorism becomes the most attractive means, well-adapted to the contemporary information environment, allowing the exploitation of the facilities provided by cyberspace to the benefit of terrorist organizations. Thus, the Internet becomes a place for providing the information controlled by terrorist organizations, the effects of which are perceived by people are as an amplification of the traditional terrorist threats. Moreover, the Internet becomes a tool of control and manipulation, the emotionally controlled person being encouraged to kill, to maim, to self-destruct or to cause other material damage.

We consider that this form of terrorism is much more complex than hacking itself and any cybercrime, being exploited by terrorist structures for propaganda, for obtaining financial support, for obtaining information and for ensuring private communication among the members of their organizations[1].

Gabriel Weiman[2] identified at least six different ways of using cyber space for terrorist purposes as follows:

1. *As a psychological warfare tool.* Different images are broadcast for the purpose of spreading terror among the target population (pictures or clips of hostages being beheaded – belonging to a certain nationality or to employees of a corporation, etc.).

2. *As a propaganda tool.* Terrorist organizations can advertise their actions through live shows, online and anywhere in the world. Dissemination of information facilitates the popularization of their achievements and the abatement of errors.

3. *As a financial tool*. It is known that Al-Qaeda received financial aid thanks to Bin Laden's wealth and the contribution of several non-governmental organizations through various sponsorship methods. Experts such as Jimmy Gurule are pointing to Bitcoin as an appropriate means of providing financial support to a terrorist organization[3]. The specific activities of organized crime managed by Daesh, and we are talking about gasoline smuggling, can be part of this type of sponsorship if payments are made with crypto-currency.

4. *As a recruitment tool.* Using the Internet, Daesh has multiplied the number of foreign fighters in comparison with what Al Qaeda held. The massive distribution of images and videos showing the "correct" mujahedin's life and the success of Daesh's actions against non-Muslim enemies (including human executions) among the population helped opening information and recruitment offices around the world. The success of these methods, as expected, has proved to be of real interest among young Muslims.

5. *As a tool to hide the organizational system and their leadership*. Practically, the hierarchy and manner of organization of the terrorist groups could be concealed by building up real networks of communication. Thus, at present, the importance of leadership through a vertical hierarchy was blurred by horizontal network leadership. Members or terrorist groups have been able to support each other, have been able to coordinate and plan attacks etc., in a cheaper and safer way. In Al Qaeda, all the "jihad brothers" were called to use the PalTalk service in order for leaders not to be detected.

6. *As a documents storage place*. On the Internet, on the web pages, we can find numerous manuals and guides on how to build explosives, about urban fight, guerrilla and survival tactics etc. The aspects that we consider essential for the activity of cyber terrorism, which we identified by analyzing the most frequent contemporary terrorist events, were grouped in the next four categories. Given that most of the information comes from open sources, where information does not always have a great level of credibility, we need to say that this ranking is based on information identified in various reference sources and the personal

interpretation of hypothetical possibilities of attack from cyber terrorists.

Cyber espionage

Cyber espionage is one of the most important and intriguing international issues of contemporary society. Current reality confirms that an information system should no longer be protected only against those identified or self-named as "bad boys," but against anyone who deliberately or accidentally enters in the comfort zone of the target. That is why one of the biggest problems of the government is the definition of cyber espionage. Many organizations have created their own definition that usually refer to factors that can cause data and information destruction during an attack on a computer network, or that hide the identity of the attacker or the way the stolen information was used etc.

In our analysis we start from the definition to be found in Tallinn Manual 2.0, which is also accepted in NATO. Starting with 2013, the provisions under Rule 32 specify that cyber espionage is "any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party." In the manual, this definition is only valid at peacetime and regulate legal relationships among state actors. Moreover, cyber espionage must be distinguished from computer network exploitation (CNE) activities. Apparently, we should not approach this definition when we talk about cyber terrorism as a sample of asymmetric warfare. Yet, the Tallinn Manual outlines some of the expert groups' conclusions that the Al-Qaeda attack on the US on September 11, 2001, is assimilated from the international legal point of view to the self-defence right to an armed attack[4], a situation that allows us to continue to use it.

Our analysis becomes more complicated when we overlap the definition with the conclusions of "Snowden" case, in which Edward Snowden has shown that anyone can spy, the Internet offering a high level of anonymity. A lot of data and information can be purchased from mobile devices connected to various Internet services, such as: iPads, tablets, mobile phones, smartphones and more. All these devices can be simultaneously in multiple relations, in various cyber and communications networks. Although there are legal provisions for sanctions an interception of cellular phone calls, it has been proven that organized crime structures and even some governmental structures can intercept and monitor calls of mobile phones. When the phone is used, a digital network allows tracking the geographic location of that device, identified under a cellular phone number; allows the activity to be determined while moving between cell sites and on the Internet etc.

Under these circumstances, nothing prevents terrorists from using the same techniques. Cyber-espionage can therefore also be used to support terrorist acts. It provides: facilitating unauthorized access; intercepting data packets; infecting computer systems with viruses; blocking the data communication process; software piracy; cloning of electronic payment devices; social engineering activities; identifying work schedules and behavioral patterns of the target etc.

From a security perspective, the risks and implications of a major cyberattack with terrorist origins can be comparable to those of the Cold War. By extrapolating these risks to a much higher degree of national or multinational interest, we will notice that procedurally nothing changes. For example, electricity network infrastructures, water treatment facilities, rail and road management nodes, air-port facilities etc., are all vulnerable to cyber espionage and other information threats. Cyber espionage can prepare for directly hitting the targets, it can provide information in support of malicious actions which are not aimed at initiating a direct attack and it may extract information to blackmail the target and obtain funds.

It is obvious that for this approach there is a need for a real force in these field, a specialized capability that, as far as we know, does not exist in the organization of any contemporary terrorist structure. However, this reality does not have to "encourage" us too much. The lessons learned let us know that when a powerful terrorist leader has enough funds and wants to buy something on the black market, he may get anything. Having money gives one the possibility to buy the services of individuals recognized as having real performances in on-line criminal activity or supporters of terrorist ideologies, good specialists in using cyber espionage instruments. By stimulating their pride, they might „solve" all the information objectives set.

Cyber frauds committed in support of terrorist activity

According to the Romanian Criminal Code, computer fraud is "the introduction, modification or deletion of computer data, the restriction of access to such data or the denial of any kind of computer system functioning in order to obtain a material benefit for oneself or for a third party, if damage was caused to a person"[5]. As we can see, this definition does not involve any link with terrorism. The definition refers to a crime specific area.

Nowadays, more and more criminals, in order to commit criminal activities outside physical or geographic boundaries, exploit the speed, the comfort and anonymity offered by the computer environment, seriously harming the victim, sometimes exerting threats on people anywhere in the world.

Although there is no universally recognized definition for cybercrime, criminal law enforcement practices distinguish between the two types of Internet crimes, namely:

• Advanced cybercrime (or high technology crimes) – they include sophisticated attacks against components and software programs;

• Base cybercrime – this includes those "traditional" crimes that have become "upgraded" due to the advent of the Internet. Among these, we include crimes against children, financial crimes and even some crimes related to terrorism.

Therefore, we need to underline once more that no matter how changing the nature of cybercrime due to these new trends in computer systems and networks, not all Internet crime activities are cyber-terrorism. Generally, those activities recognized as being organized by crime structures are geared towards maximizing profits in the shortest possible time. These include theft, fraud, illegal games, the sale of counterfeit medicine, etc.[6] We considered it necessary to make these assertions in order to understand that police structures are committed to neutralizing all cybercrime. To counter terrorists, they are also supported by other structures specialized in combating logistic or financial activities that support terrorism. In fact, the G7 Ministers of Internal Affairs requested, at the meeting in Ischia, Italy, in October 2017, the sharing of information from the global platform, about so-called "foreign terrorist fighters" (FTFs), data sharing and the analysis of predominantly extremist activity. At the end of this summit, the Ministers stated, through a joint statement, that they would "support the role of INTERPOL as a global platform for the exchange of information on lost and stolen travel documents, as well as for the systematic examination of international travelers, including the exchange of biometrical information and data collected on the battle space. Last but not least, they said they were committed to encouraging all states to increase the use of its databases."[7] Besides, INTERPOL has been the pioneer of information exchange for the legal support of military actions since 2005 through the Vennlig Project, in Iraq, and later through the Hamah Project in Afghanistan. The information provided by INTERPOL allows undermining the activities of terrorist groups, banning the movement of terrorist fighters to return to conflict zones, assessing risk profiles and supporting investigations necessary for the execution of related arrests.

Why all these signals of alert? Because, starting in 2018, due to worrying developments of geopolitics, ideological and technological threats that make the prevention of cyber frauds mainly an issue of protecting affairs against the new and emerging forms of financial crime, there is a series of effects affecting the national security state of a state. Thus, between 20-24 November 2017, an EMMA (European Money Mule Action) initiative directed against transnational money laundering identified nearly $ 31 million in illicit transfers connected to cybercrime funds[8]. According to EMMA, 90% of this money can be used to support the terrorist activity of groups such as Boko Haram, the Islamic State and Hezbollah. These funds come from so-called money transports and crypto-funds, the transports that the authorities say are essential for operations that make the activity move from criminal to terrorist purposes. Moreover, at the G7 meeting from April 4-5, 2019, the Interior ministers decided to improve the requirements for online social networks and platforms, so that they can withdraw content that contributes to the radicalization and the organization of terrorist attacks. Facebook, Twitter, Google, and Microsoft representatives have also been invited to this meeting. One of the conclusions of the G7 summit was that social service software should be updated and allow automatic blocking of all the terrorist content already identified, along with the establishment of emergency protocols to

immediately withdraw the terrorist content that might become viral[9].

In the case of military operations to destabilize the power of militants in Iraq, Syria, Somalia, etc., extremist groups appear to be targeting online financial crime, through radicalization financing efforts[10], for recruitment inside Western nations and, last but not least, for the acquisition of firearms required to perform individual and local attacks with limited objectives. It is estimated that in the future, Western extremists could develop various methods of obtaining funds through cybercrime to test new technologies, whose targets are explosive-loaded drones[11]. As a matter of fact, the most frequent targets of cybercrime on which terrorist activity is based are those aimed at online purchase of various materials, rental of cars and apartments and the purchase of explosive, chemical and/or biological components.

Terrorist organizations and their sponsors can use the Internet to fund these activities. The way in which terrorists use the Internet to raise funds and acquire resources can be classified into four general categories:

- Direct request – refers to the use of websites, chat groups, e-mail and targeted communications to request donations from supporters.
- E-commerce – as it is known, e-commerce can take place only on Internet, with websites that can be organized as online stores with various products and where books, audio and video recordings or other articles can be provided to supporters.
- The use of online payment devices – online payment service devices provide specialized service through dedicated sites. Also communications platforms facilitate the transfer of funds electronically between customers.
- Sponsorship from charitable organizations - fund transfers are often made by electronic bank transfer, credit card or alternative payment facilities available through services such as PayPal or Skype.

"Money laundering" is another important organized crime activity to support terrorist organizations. An example of this is the case of a hacker, Younis Tsouli, who, in the UK, washed away illicit gains from bank card theft in order to finance terrorist acts[12]. In order to do so, he turned to several methods, including transferring through electronic payment accounts online, funds being routed through several countries before reaching the desired destination. The money thus washed was used both to pay Tsouli's registration of 180 sites where al-Qaida propaganda videos were being broadcast and to acquire the equipment needed for terrorist activities to use in several countries. It seems that around 1,400 credit cards have been used to generate approximately £ 1,6 million in illicit funds for terrorist financing.

E-propaganda, education and radicalization

By exploiting the Internet, terrorist groups can "benefit" from promoting their own ideologies to incite hatred and violence, or to prepare terrorist acts, to attract supporters, to assist training etc. The information networks of home users, of businesses and institutions that allow the connection of various information technologies can be programmed to simultaneously run an attack on cyberspace in different sites of the world on a service or network connected to the Internet.

One of the most popular methods of attack is the promotion of propaganda material. Generally, Internet propaganda takes the form of multimedia communications that provide the reader with a lot of information that includes ideological or practical instructions, explanations, justifications or that promotes life-aspects in a terrorist organization. These can include virtual messages, presentations, magazines, treaties, audio or video-files and video-games etc., developed by terrorist organizations or their supporters. However, unlike the legitimate approach of a point of view, what constitutes terrorist propaganda is often a subjective assessment of all the issues presented.

Promoting propaganda is not a forbidden activity. One of the basic principles of international law on the protection of human rights includes the right to the freedom of expression. It guarantees the right to share an opinion or to distribute content that may or may not be acceptable to others (subject to limited exceptions). One of the generally accepted exceptions to this right is the ban on the distribution of certain sexually explicit material, a ban considered to be in the public interest to protect the vulnerable groups. Other exclusions required by law and proven to be necessary refer

to communications that are clearly harmful to the protection of national security and international communications and are likely to incite violence against individuals or specific groups.

As it is well known, promoting violence is a common topic in terrorism-related propaganda. This is one of the main ways that explains why the content distributed on the Internet and related to terrorism exponentially increases the audience, the audience being emotionally affected. Propaganda on the Internet may include content such as clips depicting violent acts of terrorism or their simulations, encouraging the user to engage in virtual play to act as a terrorist.

Promoting extremist rhetoric that encourages violent acts is another common trend identified on IT platforms that host extremist content on the Internet. It is obvious that this content can be distributed to the public, either personally or through physical media such as CDs and DVDs. Still, the basic one remains the Internet, a space that offers a wide range of tools consisting of dedicated websites, video, chat rooms and discussion forums, online magazines, social networking platforms such as Twitter and Facebook, popular video and media sharing sites such as YouTube, Rapidshare, etc.

Terrorist propaganda has as its main targets the recruitment of supporters, radicalization and incitement to violence. The broadcast messages will seek to convey exciting factors of pride, achievement and dedication for extremist purposes. They can be used to demonstrate the effectiveness of terrorist attacks and to demonstrate commitment and fairness to those who have provided financial support.

Other objectives of terrorist propaganda may include the use of psychological manipulation to undermine the belief of a particular individual in its social values, or to promote feelings of anxiety, fear or panic in a particular population or segment. This can be achieved through the dissemination of misinformation through rumors, threats of violence or images of acts of violence. The target audience may include direct and/or public viewers affected by the potential advertising generated by such material.

The Internet is the ideal place to establish connections and relationships with those who are interested, young people representing ideal victims, often lured by the bravado of the age, the acute reaction to whatever they perceive as obsolete and haterism. Moreover, on the basis of their Internet use abilities, young people can develop implied advertising by redistributing online content through discussions and messages in which they communicate their opinions to site administrators and/or other members. Terrorist groups have recognized the "power" of this instrument and have begun to skillfully use it. Thus, they broadcast on the same platforms messages and programs of youthful indoctrination with radical messages.

Although the extent of success of their action cannot be measured, it is clear that the Internet risks are becoming a powerful tool for recruitment and radicalization. For this, Daesh shows various aspects related to professional opportunities, family life or community membership. This method does not only target young people or people already in the recruitment process, but anyone who comes in contact with their propaganda products, either through a redirected link or pop-up notifications. The messages used are not simple narratives, but they are carefully manufactured to achieve a psychological influence with gradual effects. The way in which they will be received is influenced by several factors including: education, age, occupation, relational environment, way of approach etc.

The radicalization of a person depends on the family, emotional, political, financial context of the individual at that time and other. Nizar Trabelsi, accused of planting a bomb in a military unit in Belgium, on behalf of Al Qaeda, during the interrogation within the criminal investigation, said that the initial element that led him to join the terrorist cause was the presentation of a photos of a girl killed in the Gaza Strip, by recruiters, in 2001[13].

Assisted training through IT learning systems

We noted that terrorist organizations use the Internet also for disseminating information. Among their products, there are a series of practical guides as online manuals, audio and video clips, information and other online platforms, all providing an assisted IT-learning system. Moreover, these cyber platforms provide detailed instructions, in an extremely easy way, which is more intuitive (often in multimedia format, mainly local and

international languages), on various themes such as: the particularities of building an improvised explosive device; ways of using firearms or white weapons, or other improvised weapons; methods of combining some currently non-hazardous substances and transforming them into poisons or other dangerous elements; details of the planning and organization of terrorist attacks, etc.

Therefore, the cyber-training platforms thus created can be considered virtual training camps, where physical training is executed individually with or without specialized assistance. These platforms can also be used to discuss or distribute the observations identified in the experiments, to communicate lessons learned about specific methods, techniques or operational knowledge, all for terrorist action training.

For example, the online magazine called Inspire, allegedly published by Al Qaeda, has as its primary objective the Muslims' training for jihad. This publication contains a large amount of ideological material designed to encourage terrorism, including statements attributed to Osama Bin Laden, Sheikh Ayman al-Zawahiri and other Al-Qaidae leaders or representatives.

Online training features include, among other things, tools necessary for counter-information activities, hacking and protection activities, tools to improve the security of communications links and other online connection activity, selection tools for the proposal of encryption methods and anonymization techniques. It seems that the interactive nature of digital platforms in the cyberspace, helps to consolidate those feelings of communion between individuals in different locations and geographic locations, thus encouraging the creation of networks of instructional and tactical materials exchange. Moreover, the Internet can be used not only as a means of publishing extremist rhetoric and videos, but also as a way of developing relationships, a way to seek the support of those responsible for targeted propaganda, etc.

Regarding the danger of Internet radicalization, it is worth mentioning that cyber space can be an effective environment for recruiting and educating minors, knowing that this category is significant for a large proportion of users. Propaganda distributed in order to recruit minors can take the form of cartoons, popular music and videos, or computer games. As a rule, propaganda products run on websites under the control of terrorists or their affiliates and are aimed at being viewed by minors. That is why they include a mixture of cartoons and stories with certain messages that promote and glorify various acts of terrorism, such as martyrdom and suicide attacks.

Other terrorist structures create and promote digital games. Their online nature turns them into real recruitment and training tools. Such games can promote any kind of violence against a state or a certain individual for a political party; they can set scales of value and other rewards for the "success" of going through the virtual stages, and they can be offered to a wider audience often being translated in several languages for the geographical area of interest.

On the basis of the above, we can see that Brenton Tarrant's attack could be part of an online training step. The video images simultaneously broadcast on the Facebook network, *pay attention* – the images were produced and posted live by the attacker through a video camera permanently on, showed how, on March, 8, 2019, he was driving a car to a mosque, he entered the building and open fire on those inside, in a non-discriminatory manner. Later, he was shown executing the wounded fallen in the street, changing his guns, shooting people in the street from behind the windshield, and the fact that he did not open the windows while driving.

It is clear that the event was a terrorist attack, supported by the "manifesto" published on the Internet denouncing immigrants as invaders. The Internet, Facebook, Twitter, and Google have enabled many talks and the broadcast of extraneous content materials on their platforms as a result of distributing video and video products from this event. Daily Mail, quoting Clement Thibault, an analyst on the global financial markets platform Investing.com, noted that". The live-streaming of New Zealand's shooting will certainly bring on more questions of regulation and scrutiny over Facebook. It helped provide a platform for today's horrific attack and will undoubtedly be called into question for facilitating the spreading of this event"[14].

Conclusions

As we can notice, cyber terrorism must be seen as a stage in the evolution of cybercrime adapted to terrorist purposes. It is clear that the resources

provided by the cyber space and the mechanisms of cybercrime are intermingled, being exploited to the fullest by the people from both the cybercrime and the terrorist area.

From the point of view of the development of cyber terrorism, we consider that three basic scenarios can occur, the differences between them deriving from different causal relationships. We do not rule out the possibility of others, but we consider them derivatives or solutions adopted according to the resources available and the training in this field.

The three scenarios for the development of cyber terrorism are the following:

Scenario 1 – Training traditional terrorists in hacking;

Scenario 2 – Enrolling hackers for organizing and executing terrorist attacks with IT devices aid and information support from the Internet, attacks similar to "cyber mercenaries";

Scenario 3 – Attracting hackers who share the ideologies of the terrorist organization and then become active members of it.

The main methods used in the sphere of cybercrime and which could be exploited for the purposes of terrorist attack are the following: password attacks; network access attacks and data packet interception; trusted access attacks; IP spoofing; attacks through social engineering; sequence number prediction attacks; attacks with hijacking of the session; attacks exploiting the weaknesses of technology; attacks exploiting shared libraries etc. All these methods can set up a criminal purpose serving and disclosing the exact motivation for which they were launched.

We conclude that there is no difference between the necessary knowledge and the set of tools used by hackers and cyber terrorists, the effects of completing the attack and its motivation being the only elements that differentiate them. The synergy of conventional terrorism means and the information warfare is very dangerous and, at the same time, an asset for terrorists because it combines lethal goals with the main purpose of fear generation. For cyber terrorists, the adoption of these information measures allows for free action in various geographic areas, in violation of the conventional physical boundaries of contemporary states. At the same time, traditional terrorists can use the information warfare to limit the cost of such an attack, as compared to a conventional attack. Thus, using information warfare, the "low cost/increased effects" ratio is far more attractive to terrorists that use it than to those who oppose it.

Cyber terrorism is neither information warfare nor an accumulation of cybercrime. It is something new, extremely versatile, which may overlap other socio-cybernetics shapes and has great potential for development. The way terrorists will adapt their methods and techniques to the information environment requirements will remain just an option for the management of the respective terrorist organization.

NOTES:

1 Manuel R. Torres Soriano, *Guerras por delegación en el ciberespacio -Proxy wars in cyberspace*, at http://revista.ieee.es/index.php/ieee/article/download/309/473, accessed at 15.10.2018.

2 Gabriel Weimann, *How modern terrorism uses the Internet*, United States Institute of Peace, at https://www.usip.org/sites/default/files/sr116.pdf, accessed at 14.09.2018 and 16.10.2018.

3 Apud Jimmy Gurule, în Dru Stevenson, *Effect of the national security paradigm on criminal law*, at https://law.stanford.edu/wp-content/uploads/2018/03/stevenson.pdf, accessed at 16.10.2018.

4 *Ibidem.*

5 *** https://legeaz.net/noul-cod-penal/art-249, accessed at 15.02.2019.

6 Uptin Saiidi, *Inside Interpol's Singapore cybercrime-fighting complex*, at https://www.cnbc.com/2017/05/17/inside-interpols-singapore-cybercrime-fighting-complex.html, accessed at 16.02.2019.

7 *** *G7 Ministers call for sharing of battlefield data on terrorists via INTERPOL*, at https://www.interpol.int/News-and-media/News/2017/N2017-144,accessed at 16.02.2019.

8 Liam Tung, *Australia helps EU in latest crack down on money mules*, at https://www.cso.com.au/article/630544/australia-helps-eu-latest-crack-down-money-mules/, accessed at 12.01.2019.

9 *** *G7 Interior Ministers Meeting: What are the outcomes?*, at https://www.elysee.fr/en/g7/2019/04/06/g7-interior-ministers-meeting-what-are-the-outcomes, accessed at 12.07.2019.

10 Timothy L. Quintero, *The Connected Black Mark.et: How the Dark Web Has Empowered LatAm Organized Crime*, at https://www.insightcrime.org/news/analysis/connected-black-market-how-dark-web-empowered-latam-organized-crime/, accessed at 12.01.2019.

11 *** *Threat Lens 2018 Annual Forecast*, at https://

worldview.stratfor.com/article/threat-lens-2018-annual-forecast-excerpt, accessed at 12.01.2019.

12 Michael Jacobson, *Terrorist Financing and the Internet*, în Studies in Conflict & Terrorism, at https://www.tandfonline.com/doi/pdf/10.1080/10576101003587184, accessed at 10.11.2018.

13 Melodie Bouchaud, *Belgium Condemned Over Unlawful Extradition of Terrorist to the US,* at https://news.vice.com/en_us/article/3kegx3/belgium-condemned-over-unlawful-extradition-of-terrorist-to-the-us, accessed at 3.11.2018.

14 *** https://www.dailymail.co.uk/news/article-6814269/Facebook-shares-drop-execs-quit-Christchurch-live-stream-shooting-stirs-outrage.html, accessed at 15.04.2019.

BIBLIOGRAPHY

*** *Anders Breivik, autorul atacurilor din Norvegia, ar putea primi „impresionanta" pedeapsă de 30 de ani de închisoare!,* at http://www.ghimpele.ro

*** *Cyber-attack: US and UK blame North Korea for WannaCry*, at https://www.bbc.com

*** *Decret nr. 212 din 31 octombrie 1974 pentru ratificarea Pactului internațional cu privire la drepturile economice, sociale și culturale* și Pactului internațional cu privire la drepturile civile și politice, in B.Of. nr. 146/20 noi. 1974, at http://www.cdep.ro

*** *Efectul Breivik: Circa o sută de norvegieni vor să devină „terorişti solitari"*, at http://www.financiarul.ro

*** *Facebook shares drop execs quit Christchurch live stream shooting stirs outrage*, at https://www.dailymail.co.uk

*** *G7 Ministers call for sharing of battlefield data on terrorists via INTERPOL*, at https://www.interpol.int

*** *Hacked: The Bangladesh Bank Heist*, at https://www.aljazeera.com

*** *Noul cod penal*, at https://legeaz.net

*** *Threat Lens 2018 Annual Forecast*, at https://worldview.stratfor.com

Bălan George, *Noua concepţie internaţională de acţiune doctrinară şi practică în combaterea terorismului*, at http://fs.legaladviser.ro

Bouchaud Melodie, *Belgium Condemned Over Unlawful Extradition of Terrorist to the US*, at https://news.vice.com

Bumiller Elisabeth, Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, at https://www.nytimes.com

Fedotov,Yury, *Taking action where we can to stop cybercrime*, at https://www.unodc.org

Flynn Matthew J., *Is There a Cyber War?*, Excelsior College, National Cybersecurity Institute Journal, Vol. 1 Issue 2, 2014, pp. 5-7.

Jacobson Michael, *Terrorist Financing and the Internet*, in Conflict & Terrorism Studies, at https://www.tandfonline.com

Jurj-Tudoran Remus, *Instigarea publică la săvârșirea unei infracțiuni de terorism și libertatea de exprimare în practica Curții Europene a Drepturilor Omului*, at http://revistaprolege.ro

Quintero Timothy L., *The Connected Black Market: How the Dark Web Has Empowered LatAm Organized Crime*, at https://www.insightcrime.org

Saiidi Uptin, *Inside Interpol's Singapore cybercrime-fighting complex*, at https://www.cnbc.com

Schmitt Michael N. (general editor), Liis Vihul (managing editor), *Tallinn Manual 2.0,* On the International Law Applicable to Cyber Operations, Cambridge, University Press, 2017.

Soriano Manuel R. Torres, *Guerras por delegación en el ciberespacio – Proxy wars in cyberspace*, at http://revista.ieee.es

Stevenson Dru, *Effect of the national security paradigm on criminal law*, at https://law.stanford.edu

Tanasă Remus, *Benedict Anderson şi destinul „Comunităţilor imaginate"*, at https://www.lapunkt.ro

Tung Liam, *Australia helps EU in latest crack down on money mules*, at https://www.cso.com.au

Weimann Gabriel, *How modern terrorism uses the Internet*, United States Institute of Peace, at https://www.usip.org