HADMÉRNÖK

XIII. Évfolyam 2. szám – 2018. június

THE CHALLENGES OF THE CYBER-TERRORISM

A KIBERTERRORIZMUS JELENTETTE KIHÍVÁSOK

KASZNÁR Attila

(ORCID: 0000-0002-5498-0855)

kasznar.attila@uni-nke.hu

Abstract

Referring to the cyberspace it is easy to state that the application of the new structural and technological innovation have become more important. As the experience shows the terrorists use the cybertools more and more frequently in their activities. The use of the new tools by the terrorist communities means new challenges. It is highly important in the struggle against terrorism presenting modern asymmetric characteristics the services countering terrorism could set out responses appropriate to the new challenges.

Keywords: *terror, cyber-defense, security, national security, intelligence, radicalization*

Absztrakt

A kibertérrel kapcsolatosan, kijelenthető, hogy a terrorelhárításban fontossá vált a struktúrális és technológiai újítások alkalmazása. A tapasztalatok szerint a terroristák egyre gyakrabban használják fel a kibereszközöket tevékenységük során. A terrorközösségek új típusú eszközhasználata számos új biztonsági kihívást teremt. A modern, aszimmetrikus jellegzetességeket magán viselő harcban különös fontossággal bír, hogy a terrorelhárításban részt vevő szolgálatok az új kihívásokhoz igazodó válaszokat fogalmazzanak meg.

Kulcsszavak: *terror, kibervédelem, biztonság, nemzetbiztonság, felderítés, radikalizáció*

A kézirat benyújtásának dátuma (Date of the submission): 2018.03.27.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.15.

INTRODUCTION

No doubt, the cyber-threat is a determining problem of the post-modern security policy. The development in the field of technology and mostly in the information technology of the last decades gave new opportunities to the terrorist organizations what they successfully incorporated into their operational methods. The consequence is that the cyber-threat today is one of the most significant challenges in the field of national security and counter-terrorism what confirms the theory that the opportunities offered by the development of the information technology is actively used by the terrorist organizations to widen and to improve their capabilities.

It is also clear that in spite of the growing post-modern threat it seems that the expected and necessary threat awareness in the field of defense is still missing. This awareness is imminent in complex, in the individual corporative and social fields and impacts the law-enforcement and national security sectors.

The threatened ambience which is much more difficult to detect and control in a traditional society created by the widening and daily use of the cyberspace induces a plenty of difficulties never seen before in the tasks of counter-terrorism. Given that "*the asymmetric warfare becomes more and more sophisticated and efficient*" [1, p.131.] thus the integration of the cyber tools into the terrorism goes organically therefore the cyberterrorism can be considered as a step forward on the way of evolution of the terrorism. The new challenges generated by these new steps require the elaboration of new responding mechanisms because the responses elaborated for the previous status of security ambience are not efficient or can be applied only partially. The reason is that the cyberterrorism does not include the classic terrorist attacks against computer networks but it also includes the information terrorism, i. e. the homepages spreading background ideologies for terrorist acts. [2]

The problem has been recognized and its highest level consideration is also expected. The best proof for it is he current National Security Strategy which specially underlines the importance of the cyber security as follows: "*The functioning of the state and the society - in many other fields beside the economy, public administration and defense - is more and more based on computer technology. We have to consider more urging and complicated challenges in the informatics and in the telecommunication networks and in the related critical infrastructure's physical and virtual space. It is a special threat that the results of the scientific and technological development accessible for everyone some states or non-state groups – even terrorist ones – can use to disturb the ordinary functioning of the informatics and communication systems and of the governmental backbone networks.*" [3] It is hopeful that the strategy makes it univocal the political decision-makers also recognized the problem although the daily experience shows that in huge parts of the society there are complicated deficiencies which can bring to dangerous situations.

THE CHALLENGES OF THE CYBER-TERROR

The primary challenge is the prevention itself i. e. the changes happened during the intelligence work because "*The term cyberterrorism is becoming increasingly common in the popular culture, yet a solid definition of the word seems hard to come by.*" [4, p.3.] The opportunities of the counter-terrorist intelligence can widen in many aspects as a consequence of the broad opportunities offered by the cyberspace. At the same time the difficulties in this new realm appear enhanced because the cyberspace and the tools used there not only make easier the daily life and make simply the solution of the problems in general but they can cause security risks too. The assistant professor of the John Jay College of Criminal Law of the New York Municipal University says: "*It would cause serious confusion and huge inconvenience in the communication sector and would shock the whole technical culture of the society.*" [5, p.449.]

The functional models of processes univocally show that as a result of the social interactions provoked by the terrorist acts some feedback emerges what in its turn creates new inputs generating new turns of processes. We should not ignore these processes are already the result of a new psychological ambience which can be considered as a secondary effect of the terrorism. It can create deeper breaches than the primary effects. "*This secondary psychological influence on the target of the terror is the instrument which the terrorist wants to manipulate the decisions and policy of the adversary with.*" [5, p.240.]

The cyber-terrorism fits the model above and due to its specific features it parallel has the primary and secondary characteristics of the mechanisms of effect of the terrorists' tools. Thus it is an ideal tool for all terrorists, individuals or groups equally. The cyber-terrorism in every case shall be interpreted as one of the processes of terrorism therefore we have to take into account the possible inputs generated by terrorist challenges. In order to combat terrorism we have to optimize up to the maximum and to hold the manageability these new inputs.

At this point we can see the new challenges in the field of intelligence. As the result of the IT development it is univocal that the opposite communities – the terrorist groups – have opportunities never seen before like the anonymity, the non-stop access and use of the connecting services or the implementation of acts combining the endless illegality and legality through the dark web. This idea is confirmed by Gabriel Weiman, who is a Full Professor of Communication at the Department of Communication at Haifa University, Israel. Weiman considers the "*cyberterrorism is more anonymous than traditional terrorist methods.*" [6, p.6.]

All these factors listed above leads to the conclusion that chances of information gathering of the counter-terrorist services can face new obstacles. It does not mean their operational space reduces too; as much as they lose as much they gain. The opportunities change therefore in the new ambience the words said by Mark M. Loewenthal, the former head of analysis of the Central Intelligence Agency gain new importance: "*the capability of gathering information about the target can exist and cannot exist. Once it exists it can be successful or can be not.*" [7, p.498.] Although Loewenthal's words seem to be evident they can be perfectly interpreted in the unbelievably fast changing world of the cyberspace.

The challenges have extreme dynamism so the countering activities must also be as dynamic. This requirement can cause serious difficulties for the countering services operating in the traditional structures. The special feature of the difficulties is that they always have temporary character because the responses given to the new challenges partially or entirely solve the problem. We shall not ignore that the output converts into input during the feedback i. e. a new turn of difficulty can appear as part of the cyclic phenomenon already described above. Here is the short list of the main features of the new challenges as the result of the use of cyberspace by cyberterrorists:

1. Global opportunities,
2. Opportunities granted by the abundancy of information,
3. Opportunities granted by the ground informatics system,
4. Opportunities granted by the internet media,
5. The internet as a tool and venue of the terrorists' attack.

No doubt, the terrorism has become a global problem for today and the following definition is univocally true: "*it differs from all other crimes because on one hand it is ideologically and politically, and on the other hand it has global character, thus it crosses continents and state borders.*" [8, p.8.] The post-modern terrorism with its existence has the chance of being a borderless phenomenon what is enhanced by the existence of the cyberspace. The most powerful platform of this background base is the internet what basically changed the capabilities of the terrorist communities giving wide opportunities for them to appear. From the point of view of the counter-terrorism the best example are the new forms of radicalization

spread through the internet what can be seen in transferred sense as "*the main road and railroad network of the electronic world which enables a highly efficient transfer and also can reach persons living far from each other and also capable to influence their community and world perception.*" [9, p.100.] Exactly this feature of the cyberspace enabled it to be the main venue of the radicalization processes confirming the opinion of the researches of terrorism that *"the threat of the growing and horizontally also spreading radicalization, its methods and tools of persuasion to attract new followers and the methods of communication also change and become more conspired.*" [10, p.157.] Having immeasurable dimensions the cyberspace or more precisely the internet makes possible the more sophisticated, better conspired spread of radicalist teachings thus makes more difficult to discover or dismantle this process. Maintaining the connections through protected internet channels, the fast and hidden communication helps the spread of hostile ideas giving a higher safety both to the representatives of radicalist views and the people interested in knowing these ideas.

From the point of view of counter-terrorism it is a special problem that the internet has made possible the transmission of a much higher amount of information at a much higher speed. Naturally, everybody wants to know everything but the having an excessive amount of information can lead to chaos. On one hand, among the huge amount of information the most valuable pieces can lose (at this point it is necessary to underline the importance of that the experts must perfectly distinguish the data from information and vice versa), and on the other hand the difficulties in processing and analyzing this huge amount of information can generate many further problems. Today having and "stockpiling" a growing amount of information is not a primary aim because the limitlessness of the information can detain the successful implementation of the given job. As a consequence of the previous thoughts increases the value of the professional assessment and synthetization of information.

Similar problems can be caused by the Ground Informatics System (GIS). In spite of the general opinion that the GIS is one of the most impacting achievements of the contemporary societies beside the positive effects it has certain threat for the society and the individuals as well. One of the most eloquent examples can be that based upon the satellite navigation system everyone can find and identify his or her target what can also be done by the terrorists with the same success.

The next threat on the list is the internet media. The video clips showing brutal executions, decapitations and tortures prepared and divulgated by the Islamic State at a high professional level represent something else than mere propaganda and due to their mechanism of influence they can be considered as a new sort of terrorist activity.

Last but not least the internet itself can be a target or even a venue of terrorist attack. The cyberattacks have become a daily challenge and it is highly probable that their number and effect did not reach yet the level what expects the digitalizing world in the future managed and determined by the artificial intelligence (AI). Seemingly, the newt breakthrough in the development of the information technology will be the use of the AI what in its turn will basically change the life of the mankind. It is feared that the use of AI can give almost limitless opportunities to the terrorists while it will make the intelligence and counter-terrorism tasks more difficult than ever.

SUMMARY

The development of technology mostly in the field of informatics has brought significant changes into the security ambience of the first half of the 21st century putting in the focus a huge number of risk factors which have never featured even on the periphery before. As its consequence "*the dependence of the majority of societies from the online infrastructure also means a real vulnerability vis a vis the cyberattacks.*" [11, p.309.]

Concerning the cyber threat the idea that the majority of the countries are defenseless against the new security challenges is also true. The societies hardly can face or cannot face at all the security challenges of the 21st century. The problems emerge on a wide range because the population is as unprepared like the public administration. At the same time it is important to see that the preparedness and the related protection capability appear as the result of a studying process. Therefore the society sooner or later will dispose of the tools countering the new challenges but the circumstances of the formation of this capability have vital importance.

The researches related to the cyberspace and to "*the use of information technology by terrorist groups or individuals to achieve their goals*" [12, p.59.] confirm the importance of the use of structural and technological innovations to successfully face and struggle against the new security risks of the terrorism. Beside the new risks it is important to have in mind, what Dorothy E. Denning, researcher of information security of the University of Michigan said: "*terrorists have moved into cyberspace to facilitate traditional forms of terrorism such as bombings.*" [13]

The successfulness of the intelligence can be increased if the law-enforcement control over the world net can be deepened parallel to the implementation of the legal guaranties. In its turn, the development of the information-gathering mechanisms directly depends on the development of the analytical and assessment capabilities.

There is a clear tendency that the protection of the cyberspace is one of the most important tasks from the point of view of national security. The development and spread of the information technology has created brand new tools used by the persons and groups representing extreme ideologies especially by the terrorist communities. Applying these tools these terrorists change the security ambience from the roots. The internet and its special applications facilitate the radicalization to go on faster, in a wider community and giving less possibility to dismantle it. The social pages and other communication tools can have only one difficulty in transmitting extremist ideologies; the language. The activities of the las period of the Islamic State demonstrate that the internet gives an excellent propaganda forum for the terrorist groups which make increasing efforts to use it more professionally. Another special problem is the intention of terrorist groups to perpetrate cyberattacks. If these attacks end successfully for the terrorists they can cause material and moral loss which will have hardly calculable demoralizing and shocking effect in the deeper strata of the public opinion. Obviously, the primary task of the counter-terrorist services is the detection, assessment of the real or potential threats in the cyberspace and to set up the priorities among these threats.

"*The idea that both the technical development and the social changes modify also the strategic ambience including the tools using the wars, is neither sophisticated nor new.*" [11, p.316.] The basic and strategic changes in the global terror require the basic change of views in the field of counter-terrorism as well. The past decades proved "*the forces, the tools and methods used in the past could not impede the preparation of new attacks by the international terrorism, therefore forces with higher level of preparation, tools with enhanced efficiency and more successful combat methods are required in the struggle against it.*" [14, p.201.] The terrorist organizations representing a new sort of threat are not only well financed but they are also open for the implementation of the new technical solutions. [4, p.9.] The contemporary terrorism using cyber tools and its deep social embeddedness and the use of artificial intelligence in the future can create a flexible sociological status with unforeseen changes which require the urgent change of the traditional static based activities of the national security and counter-terrorist services for more successful methods taking actively into consideration the daily changes.

The conclusion of the present study is that "*the cyber security and the cyber threat are one the main security challenges of the forthcoming decades.*" [15, p.27.]

BIBLIOGRAPHY

[1] TOMOLYA J. - PADÁNYI J.: *A terrorizmus és a gerilla-hadviselés azonosságai és különbségei*; Hadtudomány 2014. 1. pp. 126-154.

[2] KOVÁCS L.: *Kiberterrorizmus*; Hacktivity 2007 Előadás. www.zmne.hu/dokisk/hadtud/terror/lekt_Kovacs_Laszlo.pdf (Accessed: Jan 15, 2018)

[3] 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról

[4] GORDON, S.: Cyberterrorism? https://www.symantec.com/avcenter/reference/cyberterrorism.pdf (Accessed: Feb 15, 2018)

[5] MARAS, M-H: *A terrorizmus elmélete és gyakorlata*, Antall József Tudásközpont 2016.

[6] WEIMANN, G: *Cyberterrorism - How Real Is the Threat?*; United States Institute of Peace Special Report. https://www.usip.org/sites/default/files/sr119.pdf (Accessed: Jan 14, 2018)

[7] LOWENTHAL, M. M.: *Hírszerzés*; Antall József Tudásközpont 2017.

[8] HANKISS Á.: *Vékony jégen*; Arc és Álarc 2017. 1. pp. 83-100.

[9] ROLINGTON A.: *Hírszerzés a 21. században – A mozaikmódszer*; Antall József Tudásközpont 2015.

[10] BÁCS Z. Gy.: *Turizmus és biztonság: turizmus a terrorizmus árnyékában*; In: GONDA T. (Eds): *A Kárpát-medence turizmusának és vidékfejlesztésének aktuális kérdései: Tanulmányok a turizmus és a vidékfejlesztés témaköréből*; PTE, Kultúratudományi, Pedagógusképző és Vidékfejlesztési Kar 2016. pp. 150-160.

[11] DANNREUTHER R.: *Nemzetközi biztonság*; Antall József Tudásközpont 2016.

[12] BOGDANOSKI, M. – PETRESKI, D.: *Cyber terrorism – global security threat*; International Scientific Defence, Security And Peace Journal 2013. July. pp. 59-72.

[13] DENNING, D. E. (2000): *Cyberterrorism*; http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf (Accessed: Jan 04, 2018)

[14] RESPERGER I.: *Kis háborúk nagy hatással: a XXI. század fegyveres konfliktusai, a terrorizmus és az aszimmetrikus hadviselés jellemzői*; Felderítő Szemle 2013. 1. pp. 200-230.

[15] HANKISS Á.: *Kiberbiztonság: az Európai Parlament feladatai*; Magyar Rendészet 2013. különszám. pp. 27-31.