RAIS | RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
December 2020

DOI: 10.5281/zenodo.4412286

Communication – a Form of Terrorist Manifestation in Cyberspace

Georgeta Stoica-Marcu

Associate Professor, PhD, Ovidius University, Constanța, Romania, daniella_gsm@yahoo.com

ABSTRACT: The internet and similar network systems are ideal for the terrorist operations they offer unprecedented communication capabilities to terrorist organizations to get their message to the world. Cyber terrorism sets out to communicate in a virtual space with threats and violent cybernetic actions. Hacker communities use this mean of communication with threats to institute cybernetic blockades, to attack various information environments of strategic importance and DoS attacks. Usually, we don't have to confound the internet (as a network) with cyberspace, which holds identities and objects that exist in networks by real individuals for different purposes. The use of communication networks by individuals offers cyberspace an emotional valence, which humanizes it. Terrorist organizations utilize the internet as a mean to communicate, mainly and have created sites on the world-wide-web to spread their ideological propaganda. The internet network, dominated by the principle of anonymity in communication is exploited to the max by the extremist terrorist organizations, which leads to feelings of anxiety, uncertainty and panic. The instruments of communication used by the terrorist organizations have evolved rapidly from the publications Voice of Jihad, Voice of Caliphate, Echo of the bloody battle and Echo of Jihad, from the television stations Al-Agsa, Hamas, Al Manar, Hezbollah and Djihad Kamal, to a communicational activity on sites and forums that they exploit intensely.

KEYWORDS: communication, Cyber terrorism, communication networks

A conclusion that resulted from the analysis of the activities organized by the main terrorist groups recently, reveals a number of 4 directions in which these organizations utilize the informatics technology.

The first would be using the internet for terrorist communications, the transforming of the communications generating a new way to command and control. The second is the access to information via the internet and world-wide-web (www), including accessing information on various targets, as well as technical data regarding weapon manufacturing.

The use of the internet as a platform to disseminate the propaganda of the groups and terrorist causes, as well as the objectives related to the recruitment of individuals in these organizations is the third direction. The fourth direction is the launch of cybernetic attacks towards various data servers that contain sensitive or strategic content.

These directions open up the horizon for my research through an analytic study of the terrorist cyberspace activities. They are completed by a series of analysis regarding information theory through a communication mediated by computer networks that define the information infrastructure. In the cyber-internet space the propaganda actions have developed in the last few years valences of promoting not only ideological ideas, but also of some activities – advertising actions, aspects that define the so-called concept of Ad-Terrorism.

According to a report of the EU, cyber-attacks are becoming more and more sophisticated and widespread. The European Union Agency for Cybersecurity (ENISA 2020) published its annual report in October 2020 in which it summarizes the main cyber threats identified between the years 2019-2020 - as shown in the official release of the EU Commission. According to the report, the attacks are constantly increasing, becoming more and more sophisticated and often left untraced. Especially, increases in phishing attacks, spam messaging and precise targeted attacks on social media platforms are being reported, in this case with terrorist origins. At a glance, they might seem harmless, but their message attracts many young people and people from different social backgrounds, as well as from different nationalities.

The EU is taking strong measures in channeling cybersecurity capabilities. In this sense it will update the legislation in the field of cybersecurity and will adopt a new cyber-defense strategy by the end of year 2020.

There is an increase of community education campaigns regarding protection against terrorist cyber-attacks and attracting youth in the online discussions. The increasingly easy access to the internet and mass-media transforms our youth into a sure target for terrorist groups that found a new way of communication and a new way to attract towards their inhumane actions. We shouldn't be surprised how much online communication can do. "Cyberspace has been, is and will remain one of the most challenging areas in the matter of national internal security" said Wolfgang Ischinger at the 2016 Security Conference in Munich (Ischinger 2016).

The focus was on the fourth industrial revolution which is connecting in a network, digitizing and automatizing the production process. The digitizing has a huge potential - say Mathias von Hein and Claudia Stefan (2016), but the participants of the Conference recognize the huge risks that come with it. In the digital world a single attacker can destroy whole "armies", added the same authors.

Transnational terrorist organizations, insurgents and jihadists have used the Internet as a tool for attack planning, radicalization and recruitment, as a method of popularizing propaganda, as a means of communication, and for disruptive purposes. Mandatory international legal instruments have not yet been developed to explicitly regulate inter-state relations in the virtual space states in opinion of Cernat (2020, 98).

As in the case of cyber warfare, there is no consensus in most national or international legislation on a definition of what constitutes cyber terrorism. Some definitions, addressing acts of terrorism that transcend borders, refer to activities and damages defined in the legislation on fraud and abuse in computer networks and systems, says the same author.

Communication in virtual space is gaining momentum, and terrorist organizations are gaining ground with online publications and forums. To these are added TV programs and radios. One cannot communicate, said Paul Watzlawick (Lesenciuc 2017, 3). WWW (World Wide Web), in translation "spider web of universal proportions", allows the distribution of information of all kinds, including terrorist propaganda.

There are also a number of disadvantages related to vision, computer addiction, overwork, and a problem that is not often circulated at the moment, reducing interpersonal communication. Studies have shown that 66% of respondents prefer the virtual world. 31% of respondents, who use the Internet, use it for fun purposes and only a few percent - for research purposes. Deepening the personality in the virtual world leads to destructive montages such as imaginative satisfaction of needs or their satisfaction with minimal effort. Thus there is "the danger of the formation of the personality alienated from the moral norms with all its consequences." Excessive use of the computer reduces "live communication" emphasizes Cojocaru (2014). It is recognized in the literature that the term cyber terrorism was first used by Collin (1997, 14-18) in his book .

In the Romanian legislation, the crime of cyber terrorism is incriminated in art. 32 para. (1) lit. q) of Law no. 535/2004 on preventing and combating terrorism, as offenses against the security and integrity of computer systems and data, if they are politically, religiously or ideologically motivated and are committed for the following purposes:

a) Intimidation of the population or a segment of it, by producing a strong psychological impact;

b) The illegitimate coercion of a public authority or international organizations to fulfill, not to fulfill or to refrain from performing a certain act;

c) Serious destabilization or destruction of the fundamental, constitutional, economic or social political structures of states or international organizations published in the Official Gazette of Romania, Part I, no. 1161 of December 8, 2004, as subsequently amended and supplemented.

The author analyzes the constituent elements of the crime of cyber-terrorism from the perspective of the Romanian legislation, with reference to the case studies reported in the public space and the specialized literature, case studies, which, although not cataloged as being terrorist attacks, can be used as a reference material for the practitioners and researchers in the field (Jurj-Tudoran 2017).

Man thus becomes a simple terminal of multiple networks (Baudrillard 1997, 12): television, telephony, social networks, etc., and not the superman who extends his nerve endings everywhere. What is offered by media technologies under the name of "communication" is in fact an obscene form of symbolic commodity. Karl Marx had already denounced the obscenity of commodity, linked to the "abject" principle of its circulation. We no longer live in the drama of alienation; we live in the ecstasy of communication (Baudrillard 1997, 15-16).

Introduction of the concept of gatekeeper

The group thus becomes a distinct organism, which functions thanks to the exchange/ communication between individuals. In this context, the group outlines specific functional schemes, which involve a specific organization of the communication flow. Lewin Kurt introduces in the study of communication within the group certain selection filters, which have become "gates", which are "guarded" by decision-makers regarding the transmission of information units (gatekeepers). Whether deliberate or not, the setting of the agenda by the media is a proven fact through research, and the shaping of the agenda is the result of a process of influence, intentionally through mass communication (Lewin 2001).

The role of Lazarsfeld's study, which mainly pointed out that "more than anything else, people are motivated by other people" (Lazarsfeld, Berelson and Gaudet 2004, 208).

The tyranny of communication

The French journalist and writer of Spanish origin Ignacio Ramonet, since 1991 editor-in-chief of Le Monde Diplomatique, is one of those who take a stand against the media offensive, amid a continuous strengthening of the role of technology. In terms of power relations, the media is no longer in fourth place, but in second place as a power of influence, after the economy and before politics.

At the same time, Ramonet draws attention to the fact that through the media "information" has lost its status, becoming a commodity. Information becomes the main player in the profit market and is no longer subject to its original purposes. What matters is the degree of interest it can arouse in the public, the ability to sell, and not the need for knowledge or novelty, aspects that are otherwise outdated.

It matters the functionality on the market, which implies the functionality of the scenarios and not the achievement of an ideal of veracity. The truth that matters is the media truth, the only one that the citizen has at his disposal to verify news, to confirm it or to deny it. Distorted information therefore becomes spectacle information. It evolves; creating a sense of unease among a society that is losing its landmarks and whose culture is being attacked by fluctuating visual images. The print media, television, the internet, accelerate the circulation of information, seductive information, which follows the "logic of suspense and spectacle". Basically, the parameters that have a decisive influence on the information are the media mimicry, the fever of which they are.

"It shows, it exhibits, it works, it 'communicates' an entire electronic actuator, it seems to tell us: 'What I show you is true, because it's technological' and we believe because it intimidates us, impresses us, takes our eyes off and convinces us that a system capable of such wonders cannot lie.", says Ignacio Ramonet (2000, 39) planetary, like a huge spider's web, taking advantage of digitalization and favoring the interconnection of all services in the field of communication and information. (Ramonet 2000, 133-134)

Returning to McLuhan's metaphor for the extension of the human nervous system on a planetary scale (McLuhan 1994), Ramonet's view is different: the human nervous system, including the neocortex, is made of prostheses that react to certain stimuli, allowing it to take certain decisions. The media is implanted in the human consciousness and keeps people captive. The tyranny of mass communication is subtly established and controls the needs, tastes, preferences, desires of the individual connected to the network through technology.

Terrorist structures have a big influence and traditionally built of loose-knit cells, divisions, and subgroup, are ideally suited for flourishing on the internet through websites, email, chat-rooms, e-groups, forums, virtual message boards, YouTube, Google Earth, and other outlets. Weimann (2015) said in his interesting book terrorism's arrival online. Recent trends - such as engaging children and women promoting lone wolf attacks, and using social media - and future threats, along with ways to counter them. Author analyzes content from more than 9,800 terrorist websites and selects their most important kinds of web activity, describes their background and history, and surveys their content in terms of kind and intensity, the groups and prominent individuals involved, and their effects. Weimann also considers cyberterrorism against financial, governmental, and engineering infrastructure; efforts to monitor, manipulate, and disrupt terrorists' online efforts; and worrisome threats to civil liberties posed by ill-directed efforts to suppress terrorists' online activities.

In **conclusion**, we can remark communication is a form of terrorist manifestation in cyberspace when "spider web of universal proportions", allows distributed a lot of information for all kinds, including terrorist propaganda and how wonderful Paul Watzlawick one cannot communicate said.

References

Baudrillard, J.1997. *Celălalt prin sine însuşi (The Other, by himself).* Translate by Ciprian Mihali. Cluj-Napoca: Casa Cărţii de Ştiinţă Publishing House.

Cernat, R. 2020. *Războiul cibernetic și terorismul cibernetic - trăsături și răspunsuri la aceste amenințări (Cyber warfare and cyber terrorism - traits and responses to these threats.).* Romanian Military Thinking Journal, no. 3: 98, Available at: http://gmr.mapn.ro/app/webroot/fileslib/upload/files/arhiva%20GMR/2020%20gmr/3%202020%20gmr/CERNAT.pdf.

Cojocaru, V. 2004. *Schimbarea în educație și schimbarea managerială (Change in education and managerial change).* Chişinău: Lumina Publishing House.

Collin, Barry C. 1997. "The future of cyberterrorism: Where the physical and virtual worlds converge." *Crime and Justice International* 13 (2): 14-18.

ENISA (The European Union Agency for Cybersecurity). 2020. "ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected." https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.

Ischinger, W. 2016. Munich Security Conference. Welcome Remarks, available at https://securityconference.org/en/medialibrary/asset/ welcome-remarks-by-wolfgang-ischinger-1400-12-02-2016.

Jurj-Tudoran, R. 2019. "Infracțiunea de terorism cibernetic – elemente constitutive și studii de caz (The crime of cyber-terrorism). In *Juridice.ro.* https://www.juridice.ro/658479/infractiunea-de-terorism-cibernetic-elemente-constitutive-si-studii-de-caz.html.

Lazarsfeld, P.F., Berelson, B. and Gaudet, H. 2004. *Mecanismul votului. Cum se decid alegătorii într-o campanie prezidenţială. (The People's Choice: How the Voter Makes Up His Mind in a Presidential Campaign).* Translate by S. Drăgan. Bucharest: Comunicare.ro Publishing House.

Lesenciuc, A. 2017. *Teorii ale comunicării (Communication theories).* Braşov: Academia Forţelor Aeriene „Henri Coandă" Publishing House.

Lewin, K. 2001. "Frontiere în dinamica grupurilor. Canalele vieţii de grup, planificarea socială şi cercetarea-acţiune. In Pierre de Visscher, Neculau A. (coord.). 2001. *Dinamica grupurilor. Texte de bază. (Group dynamics. Basic texts).* Iaşi: Publishing House Polirom.

Mathias von Hein and Stefan C. 2016. https://www.juridice.ro/658479/infractiunea-de-terorism-cibernetic-elemente-constitutive-si-studii-de-caz.html.

McLuhan, M. 1994. *Understanding Media: The Extensions of Man*. Cambridge, MA: MIT Press.

Ramonet, I. 2000. *Tirania comunicării (Tyranny of Communication)*. Translate by Matilda Banu. Bucharest: Doina Publishing House.

Weimann, G. 2015. *Terrorism in Cyberspace: The Next Generation* Woodrow Wilson Center Press with Columbia University Press.