International Relations

MANIFESTATIONS OF CONTEMPORARY TERRORISM: CYBERTERRORISM

Gabriela LUCA[1]

ABSTRACT: THE ANALYSIS FOCUSES ON ONE OF THE MOST IMPORTANT THREATS TO WORLD SECURITY AND A NEW AND EMERGENT FORM OF TERRORISM THAT USES ADVANCED COMPUTING TECHNOLOGIES IN ORDER TO DISRUPT CRITICAL INFRASTRUCTURES. FIRST OF ALL, THIS PAPERACKNOWLEDGES THE IMPORTANCE OF TECHNOLOGICAL ADVANCEMENT AS BOTH FOR THE SECURITY AND FOR TERRORIST MEANS. AND SECONDLY, IT DISTINGUISHES BETWEEN WHAT CAN BE CONSIDER A CYERTERORIST ATACK FROM A THEORETICAL PERSPECTIVE ANALYZING THE BASIC ELEMENTS AND DISTRIBUTION OF CYBERTERORIST CAPACITIES. THIS RESEARCH ALSO PRESENTS THE POTENTIAL OF IMMINENT AND ONGOING ATTACKS AND HOW THIS TYPE OF TERRORISM COULD PROF TO BE MORE DISASTROUS AS ANY OTHER KIND. IN THE END OF THIS ANALYSIS WE WILL PROVIDE EVIDENCE OF SUCH ATTACKS AND WE DISCUSS SCENARIOS THAT ARE LIKELY TO HAPPEN IN THE NEXT DECADE AND THAT COULD AFFECT THE UNITED STATES THROUGH TEMPERING WITH THE POWER GRID.

KEY WORDS: SECURITY, CYBERTERRORISM, INTERNET, AL-QAEDA, INTELLIGENCE, CRITICAL, INFRASTRUCTURE, TECHNOLOGY,

INTRODUCTION

The current century is important from a historical point of views due to the technological revolution. What was early a utopia last century and S.F. idealism today is a reality? Interconnection and the facility to obtain information have changed the world in an accelerated way that was not been previously anticipated. This development has caused both economic growth and a political and geopolitical streamline communication.

If in the 1970s the predominant viewpoint was that of an Informatics Society, a concept that gradually gained more ground and became a reality with the explosion of the Internet, the main vector of our current society, with special focus on the last decade of the twentieth century, the first part of the twenty-first century is the concept of a Knowledge Society.[2]

[1] "Mihai Viteazul" National Intelligence Academy, luca.gabriela1@yahoo.com

[2] Acad. Mihai Drăgănescu, "Societatea informaţională şi a cunoşterii. Vectorii societăţii cunoaşterii", published in "Limba Română în Societatea Informaţională-Societatea Cunoşterii", (Editura Expert, 2002), 441-442,

From the perspective of national security the internet and the computer, advancements enabled both the development of security measures and the improvement of security technologies. The global intelligence community has most benefited from this technological evolution as it is much easier to detect threats of all kinds by improving monitoring processes, information gathering, storage, and analysis.

One of the basic features of modern technology is accessibility. Without it, we could not have today's progress, but the ease with which these resources can be used often proved a significant threat. Be it cyberterrorism, cybercrime, or electronic theft and publishing of classified documents, this type of threat is becoming increasingly conspicuous and problematic.

CYBERTERRORISM AND CYBERSPACE IN THE CONTEXT OF GLOBAL TERRORISM

Cyberterrorism has become a continuously evolving phenomenon, therefore it is difficult to be defined through the increasingly blurred boundaries. The Federal Bureau of Investigation (FBI) considers this form of terrorism as a *"premeditated attack, politically motivated against information, computer systems, software and data, resulting in violence against noncombatant targets, by subnational groups or clandestine agents."*[3]

In a baseline understanding of this phenomenon, we can consider an action as belonging to cyberterrorism when an individual or an organization uses aggressive tactics and techniques, trying to intimidate or to have a noticeable negative impact on people or property.[4]

The concept of cyberspace was first launched by William Gibson and has generated the birth of a cyberculture. It had an important psychological relevance and determined the development of theoretical and research areas, such as the psychology of cyberspace and social computer science etc. These aspects focus on social, economic, and the cultural impact that the new environment of information and communication based on Internet infrastructure, generically called cyberspace, plays individually, socially, in business, science, research, education, administration and even government.[5]

Cyberterrorism can be understood as a convergence of terrorism and cyberspace. It can take many forms such as threats or attacks against computers, networks and the information stored in them, having the purpose to intimidate or coerce a government or the population into the promotion of political or social objectives. Moreover, to qualify as cyberterrorism an attack must result in violence against people or property, or at least do enough harm to generate fear. Attacks that lead to death or bodily injury, explosions or significant economic losses can be examples of such attacks.

There are numerous ways in which cyberterrorism can materialize, they tend to become increasingly diverse and difficult to classify, but there are four types of operations by which terrorists act in the virtual environment, namely:

• Penetration and serious disruption to information systems;

---

[3] Serge Krasavin, *"What is Cyber-terrorism?"*, CCRC, accessed December 12, 2016, http://www.crime-research.org/library/Cyber-terrorism.htm

[4] Matthew J. Littleton, *"Information age terrorism: toward cyberterror",* Naval Postgraduate School, Chapter 2, accessed December 12, 2016, http://fas.org/irp/threat/cyber/docs/npgs/ch2.htm

[5] Ionuț Marius Chitoșca, *"Internetul ca agent de socializare a genereției „M",* Revista de Informatică Socială, numărul 5, iunie 2006, 61

• Alteration or theft of data and information stored on machines, readable data with the stated aim of producing significant damage, economically and socially;

• Influencing political decisions;

• In response to hostile actions.

It should also be noted that there are three levels of cyberterrorist capability the world is facing, namely:

• Simple, unstructured: the ability to perform basic attacks against individual systems using tools created by someone else. This level belongs to organizations with small capacities of analysis and control.

• Advanced, structured: the ability to perform multiple sophisticated attacks on a series of networks and systems with their own tools. At this level, we find organizations with an average control and analysis capabilities.

• Complex, coordinated: the ability to perform coordinated attacks that cause severe damages against complex, integrated and security systems through personal, highly sophisticated tools. This level belongs to organizations with large resources for analysis and control.

NATO is the only international military organization that has a cyber defense department that fights to prevent cyberterrorism. This type of terrorism targets attacks on critical IT infrastructures and is becoming increasingly problematic for the Member States of the agreement. Moreover, NATO believes that a cyber-attack needs to be treated as a ballistic missile attack because both can be equally devastating[6] and included this threat as one of the three most imminent ones for the next decade (along with terrorist attacks and military attacks with ballistic missiles).[7]

Today it is considered that the desire to possess weapons for cyber-attacks is similar to the race for nuclear weapons, all nations –especially the disadvantaged ones- are trying to develop this ability in order to obtain another geopolitical balance of forces.[8]

Critical infrastructures that can be affected by a cyberterrorist attack are typically defined as being decisive for stability, security, and safety of systems and processes, with an important role in conducting economic and social, political and military processes. The degree of criticality of these infrastructures is correlated with the significant effects induced by their disturbance or decommissioning, even if just for a very short period of time.[9] We can see that indeed a cyber-attack on a critical infrastructure can be a catastrophic event for national security.

CYBERTERRORISM AS A THREAT TO GLOBAL SECURITY

Nowadays cyber security has become an issue with catastrophic implications for national security. Following a series of coordinated attacks on government institutions and even the main server of the CIA and British and Israeli security agencies, leaders of the main NATO countries consider cyberterrorism the main threat at this time. In the beginning of 2014 the company,

---

[6] Murat Dogrul, Adil Aslan, Eyyup Celik*, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism"*, Turkish Air War College, 2011 3rd International Conference on Cyber Conflict, 39, accessed December 15, 2016 as PDF,
https://ccdcoe.org/ICCC/materials/proceedings/dogrul_aslan_celik.pdf

[7] Dogrul, Aslan, Celik*, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism*….40

[8] Nicole Perlroth, David E. Sanger, " Cyberattacks Seem Meant to Destroy, Not Just Disrupt", New York Times, published March 28, 2013, accessed December 15, 2016, http://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-seek-to-destroy-data.html

[9] Serviciul Român de Informaţii, Protecţia Infrastructurilor Critice, 6, accessed May 5, 2016

Kaspersky Lab discovered the most sophisticated cyber-attack so far called "Mask". This attack was not totally stopped and is supposedly still ongoing and aimed at oil and gas companies. We must also take note of the cyber-attack called "Flame" that paralyzed the whole information system of Iran. Following this information, the U.S. president declared cyberterrorism the biggest threat and has made fighting it a priority.[10]

In October 2012, U.S. Defense Secretary Leon E. Panetta warned of an imminent "cybernetic Pearl Harbor" by showing the informational vulnerabilities and that the main objectives to be attacked in the future are the power grid, the transportation system, and the economic-financial system. On this subject former FBI Director Robert Mueller also believes that *"Stopping terrorism is our top priority but we must recognize that soon cyberterrorism will be the biggest threat."*[11]

Cyberterrorism is today the most common form of social and political sabotage. For example, in May 2007 Estonia was faced with one of the largest cyber-attacks that totally paralyzed the governmental IT infrastructure and that of the two main Estonian banks. A year later in August 2008 in the war between Russia and Georgia, three days before the invasion of South Ossetia the main TV and radio stations were blocked and the transmission was modified to transmit pro-government television channels.

Cyberterrorism is today the most common form of social and political sabotage. For example, in May 2007 Estonia was faced with one of the largest cyber-attacks that totally paralyzed the governmental IT infrastructure and that of the two main Estonian banks. A year later in August 2008 in the war between Russia and Georgia, three days before the invasion of South Ossetia the main TV and radio stations were blocked and the transmission was modified to transmit pro-government television channels.

It also needs to be mentioned that terrorism began to be promoted increasingly more in the cyberspace. Both ISIS and Al Qaeda have adapted to Western technology and methodology recruiting and motivating terrorist factions via the Internet. These attempts and methods of operation are increasingly effective and need be stopped. For instance the "elimination of Anwar al-Awlaki, considered" -Osama bin Laden main internet recruiter is a notable success of US intelligence, given his involvement in the radicalization of Muslim Americans and other English-speaking Muslims through the use modern means of communication (The Internet, social networks, etc.). Some examples of his success prior to the intervention of U.S. intelligence was: the radicalization and training of Nidal Hassan Abdul, a US army officer, the radicalization of Nigerian Omar Abdulmutallab, of British Airways, etc."[12]

CYBERINTELLIGENCE IN ROMANIA

In Romania, there is an increased risk of crimes and acts of cyberterrorism. For example FBI's most-wanted people in this domain ranks a Romanian in second.

---

[10] Christopher Harress, „ *Obama Says Cyberterrorism Is Country's Biggest Threat, U.S. Government Assembles Cyber Warriors",* accessed December 15, 2016, http://usa.kaspersky.com/about-us/press-center/in-the-news/obama-says-cyberterrorism-countrys-biggest-threat-us-government-as

[11] Senate Select Committee on Intelligence, feb 2012, accessed December 15, 2016 as PDF, https://www.amnestyusa.org/pdfs/sscistudy1.pdf

[12] Marius Lefter, *"Transformări ale războiului mondial împotriva terorismului internaţional",* Geopolitics.ro, published 02.02.2012, accessed December 15, 2015

The Romanian Intelligence Service was appointed by the Supreme Council of National Defence as the national authority in the field of Cyberintelligence in order to manage these situations. So RIS built a specialized structure called the National Cyberint Center. Its main mission is to bring together technical defense systems with informative capabilities to identify and provide legal beneficiaries with necessary information to prevent, stop and/or limit the consequences of an aggression on ICT systems which represent critical infrastructures.

RIS also admits that there are state and non-state entities with their own economic, political or military interest that causes cyber assaults. They are directed against systems of information technology and communications (ICT), which are part of the critical infrastructure itself (for example telecommunications and the Internet) or are essential for the proper functioning of other state critical infrastructure (for example air transport infrastructure, railway and roads, energy supply systems, gas, oil and water, health services, banking system etc.).

CONCLUSIONS

I started this essay assuming that without immediate solutions, cyberterrorism will produce noticeably more casualties in the coming decades than any other form of terrorism. From the arguments that were presented, I would consider this hypothesis to be confirmed; although currently to Western society the terrorist threats caused by the waves of refugees coming from the Middle East and the Mediterranean regions are still the most problematic.

Considering previous cyber-attacks and hacktivism (which even if it can't fit into cyber-terrorism troubles world governments) we can notice the potentiality of imminent further attacks on critical infrastructure networks. Also, the specialists, experts, and presidents of NATO countries led by the U.S. President Barack Obama warn about the devastating effects that cyberterrorism will have in the future.

If we were to make the effort to imagine and for example we would consider truthful Ted Koppel's view (BBC and ABC News journalist / Nightline- war correspondent in Vietnam) expressed in his new book 'Lights Out', in which he shows that an attack on the power grid of the U.S. is imminent in the next 20 years by Russia and China, which already have this capability; or the Islamic State which according to recent information seek to develop this kind of terrorism with $2 billion available funds then how many people will be affected? Considering that food and water supply depend on the power grid, it's collapse can cause tens of millions of victims. To a similar extent, we already know that cyberterrorists have the ability to lock the computer systems of banks (Estonia 2007) and if there was a globally coordinated attack, certainly dozens or even hundreds of millions of people could be affected.

In conclusion, looking at past cyberterrorist attacks and warnings from directors of intelligence and NATO commissions, we can easily see that without concrete measures, terrorist organizations and states that are opposing the proper functioning of the global socio-economic mechanisms will develop into a type of information terrorism to the point that such attacks will endanger social security and the safety of the entire world.

REFERENCES

1. **Acad. Mihai Drăgănescu**, ”Societatea informaţională şi a cunoşterii. Victoria societăţii cunoaşterii”, published in ”Limba Română în Societatea Informaţională-Societatea Cunoşterii”, Editura Expert, 2002, p.441-442,
2. **Christopher Harress,** „ *Obama Says Cyberterrorism Is Country's Biggest Threat, U.S. Government Assembles Cyber Warriors”*, accessed December 15, 2016, http://usa.kaspersky.com/about-us/press-center/in-the-news/obama-says-cyberterrorism-countrys-biggest-threat-us-government-as
3. **Dobrinoiu, Maxim**, *”Criminalitatea informatică, ed. Academiei Naţionale de Informaţii”,* Bucureşti, 2009, p.174-176
4. **Ionuţ Marius Chitoşca**, *”Internetul ca agent de socializare a genereţiei „M”,* Revista de Informatică Socială, numărul 5, iunie 2006, pag.61
5. **Marius Lefter**, *”Transformări ale războiului mondial împotriva terorismului internaţional”,* Geopolitics.ro, published 02.02.2012, accessed December 15, 2015
6. **Matthew J. Littleton**, *”Information age terrorism: toward cyberterror”,* Naval Postgraduate School, Chapter 2, accessed December 12, 2016, http://fas.org/irp/threat/cyber/docs/npgs/ch2.htm
7. **Murat Dogrul, Adil Aslan, Eyyup Celik**, *”Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism”*, Turkish Air War College, 2011 3rd International Conference on Cyber Conflict, p. 39, accessed December 15, 2016 as PDF, https://ccdcoe.org/ICCC/materials/proceedings/dogrul_aslan_celik.pdf
8. **Nicole Perlroth, David E. Sanger**, ” Cyberattacks Seem Meant to Destroy, Not Just Disrupt”, New York Times, published March 28, 2013, accessed December 15, 2016, http://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-seek-to-destroy-data.html
9. Senate Select Committee on Intelligence, feb 2012, accessed December 15, 2016 as PDF, https://www.amnestyusa.org/pdfs/sscistudy1.pdf
10. **Serge Krasavin**, *”What is Cyber-terrorism?”*, CCRC, accessed December 12, 2016, http://www.crime-research.org/library/Cyber-terrorism.htm
11. Serviciul Român de Informaţii, Protecţia Infrastructurilor Critice, pag.6, accessed May 5, 2016