# CYBERSPACE, A NEW PLAYGROUND FOR TERRORISTS

**Alexandru Ciobanu**

Ministry of Internal Affairs / Department for Intelligence and Internal Protection

**Abstract:**

Cyberspace is characterized by the lack of state borders, anonymity and dynamism. The more a State is computerized, the more vulnerable it is. Ensuring the safety of cyberspace must be a major concern of all stakeholders, especially at institutional level, where it comes the responsibility for development and enforcement of consistent policy in this field.

States that produce and export the technology in the field of cyber security, to other states, have an advantage in front of them, being able to monitor their activities and gather intelligence from areas of crucial importance, such as energy, health, economics, the military, politics and others alike.

*Keywords: cyberspace, Internet, cyber aggression, cyber warfare, terrorism, hackers*

## Cyberspace

In the field of security, 11 September is known as a day that changed everything, which marked the beginning of a new era. Our perceptions about traditional threats have collapsed with twin towers. Cold War scenario, which had dominated for more than 50 years, has been changed radically and irrevocably. The threat no longer had an clear address (national) of a sender. The borders have become meaningless, as was the case with military rules of space and time. The use of civil aircraft as instruments of a terrorist attack has shown that almost every thing might turn into a gun at any time. Suddenly, nothing seemed impossible or unthinkable. This description is almost similar to that of the phishing scams threats.

Over the last 20 years, information technology has been developed very much. From an instrument in order to optimize administrative processes by the Office, it is now a strategic instrument of industry, government or military. Before September 11, space risks and threats have risen were discussed in small groups of technical experts. But, since that day, it became obvious that the world might be assumed serious vulnerabilities for the various companies, which are increasingly interdependent.[1]

These days, for all of us, it is impossible to imagine life without interacting with the computer. Each field of human activity requires recourse to IT and communication networks, that are globally inter-connected. Connections of this kind provide a essential support in all of the areas of activity: social, economic, financial, political, and, last but not least, military and security-related issues.

Common environment in which these networks operate it is called, generic, cyberspace. This space it is not just the technological universe used by people to do what they are programed to do, to communicate with each other, but a transposition of their social reality, in a virtual environment.

Political and social impact of virtual space has been demonstrated, in a formula like no other, in the so-called *„Twitter”* or *„Facebook revolution”*, phrases used in the mass-media during the protests recorded in 2009 in the Republic of Moldova and Iran, in the election context, and subsequently in Tunisian and Egyptian episodes of the *"Arab spring"*.[2]

Cyber warfare field faced, within a very short period of time, deep changes, offering exceptional opportunities, but also risks as for its users. Sources of risk are represented by a part of the actors that populates it, which speculates, in the interests of a state ororganization, or individually, industry-specific vulnerabilities.

In the last few years, on the ground of cyber-attacks and phishing/scams-related incidents increase, attention to this kind of threats have risen and their impact on the national security is increasingly high.

We are witnessing an unprecedented extend of communications networks, determined mainly by a vast range of eye-catching network services which are available to users, miniaturization and affordability of storage resources, simplicity of use of new equipment and software performance. In proportion to these commercial offers, the number of hoem and residential users is increasing.

Nowadays, many vulnerabilities of communications networks are easily exploited, and the people and organizations everywhere are able to connect to these networks, across national boundaries. Information technology also permit to easily hide the real location and identity of the persons and organizations that take advantage of these vulnerabilities.

## Cyberterrorism

New category of criminals acting in the cyberspace is not composed of special persons or coming from space or another planet. „Cyber criminal” is more than just a name change as regards offenses traditional approach in a new shape. Digital criminals and the felonies committed by them, represent a fundamental transformation in our own way to approach the issue of crime and criminality.[3]

New categories of offenses, which is now a new type of criminality, are also committed by people, all with guilt, and take into account, as a rule, the development of economic benefits.

If we take into account the motivation and the threats presented by their actions, the cyber-criminals can be divided into groups which act on social reasons - those who have a

[1] NATO Magazine – *Noi amenințări, dimensiunea cibernetică,* http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/RO/index.htm, accessed in 05.09.2013;

[2] Intelligence Magazine, number 19, march – may 2011, pg. 3

[3] *T.Amza, C. Amza*, Criminalitatea informatica, Ed. Lumina Lex, Bucuresti, 2003.

mentality of "gang members" and want to stand out, groups acting on technical reasons - will help to develop new technologies, being a factor of technological progress, considering that, penetrating computer systems and showing their vulnerabilities, determine firms involved to force resolve them, groups set up around political reasons - those who have strong political attachments and penetrates IT systems selected on the basis of their political beliefs, to make known their views. A subcategory of this latter group is represented by the terrorists. The feature of this group of criminals is that, unlike the other categories, they are using computerised systems for both to promote terrorist actions, as well as to propagate ideas that promote hatred yes breed or hatred between some organizations, in order to incite mass of people go on a illegal social behavior.

Day-to-day occupation of this type of criminals have so far been and a wide range of jobs, they can arise from among students, specialists in various areas or belonging to organised crime or terrorist groups.

The cyber-terrorism represents convergence between cyber space and classic terrorism. Here we include: the transactions of penetration and serious disruption of computer systems, the operations of alteration or theft of the data and information stored in the various computer environments, in order to produce significant damage on the economic and social fields, and last but not least operations to influence political decisions or in response to hostile action. An example of this can be penetrating a system of air traffic control which would have resulted in a collision between two aircraft.[4]

In accordance with FBI, terrorism cyber warfare is defined as use of resources in the field of communications and informatics in order to intimidation or expedited their fellow humans.

Security incidents of IT&C shall be entered in the field of INFOSEC and they both are part in the classified and sensitive networks, as well as in the public ones. In the first category are some of the governmental networks or belonging to the state or private, as well as networks with international coverage of NATO, EU or other organizations. From the category of public networks, the Internet is the most representative and largest network, which has become a global structure (cyberspce) that connects millions of networks, hundreds of millions of personal computers, as well as a variety of mobile devices such as smartphones, tablet, PDA, etc. The global network, as well as delivering information treasury, has major role in effective operation of the various fields: business, banking, trade, public administration, even defense and national security.

But the real advantages of this user-centric ,ever-expanding architecture, smooth operation of information movement, are crashing on the other side, that of loosening of control over systems in general, and over the resources and services offered via them.

On these infrastructures, there has to be an impressive number of attempts of aggression, coming from inside or outside organizations. The cyber-attack is without frontiers, and ensuring security of the network and of the transactions by such mega-networks represetns the biggest challenge in this area.

Via the Internet, the exponents of the terrorist phenomenon can target achievement of specific objectives starting from the collection/exchange of information, propaganda, prozelitism, financing, organizational networks, and which culminated in planning/ implementation of phishing scams attacks on critical infrastructures, affecting the safety of national targeted state.

As mentioned earlier, in order to achieve cyber attacks, extremist-terrorist organizations may use attackers, with a high level of training and specialization in information systems and communications, with various intentions or reasons.

[4] *D. Denning*, Activism, Hacktivism, Cyberterrorism, pg. 241

Recruitment of such individuals constitute a constant concern for the exponents of terrorist phenomenon, as in states like China, Russia, India, North Korea or Pakistan, there are many of the people who have advanced knowledge in IT&C. Although so far, extremist-terrorist organizations such as "Al-Qaeda" or "Hamas" have used the Internet, mainly as a means of communication or at propaganda purpose and attraction of new proselytes, it is expected that in the future, with the development of their capabilities, be entitled to the cyber-attacks on critical infrastructures, which, whether or not in combination with the classic attacks, would have a strong psychological impact over the target population.

The attacks against some computerized governmental or private network, carried out so far, have demonstrated efficiency, causing both financial and institutional damages, aspect that generates attraction for such action on the part of extremist-terrorist groupss. Thus, since 1999, a group of Serbians hackers has conducted distributed denial-of service (DDoS) attacks over computerised systems of NATO, protesting, in this way, against air strikes against Kosovo and Metohija. Also, in May 2007, government computerized network activity in Estonia has been seriously disrupted after a cyber attack, event which was repeated in June 2008, in Lithuania.[5]

The advantages conferred by unforseable and invisibility (with reference to the identification of state-origin of the attack) of a cyber aggression carried out by a terrorist organization may lead to devastating results, context what steps should be taken to ensure appropriate security phishing scams.

In Romania, in the same year, under the authority of the Ministry of Communications and Information Technology, (now Ministry for Information Society) has begun to operate National Center for Response to Security Incidents of Informatics (basicly a Computer Emergency Response Team), with the aim of creating a center of excellence in the field of safety information, equipment, networks, and information systems and to focus on experts interest in IT&C environment, but also of the authorities, on the security of virtual environment.

*The main objectives of the structure are:*

- setting up a national center for the dissemination of information on security tools and guides of "good behavior" in virtual environment for the various categories of users, in the Romanian language;
- establishment of databases, regarding the incidents of security in which Romania is involved, with a view to identifying optimal measures to counteract and limitation of injury;
- provision of communications infrastructure and data bases for the security environment IT&C, as core, of an entire community of specialists in the field.

In the last 3 years, more and more states have taken steps to create a legislative framework to govern the attempt of governments to counteract potential attacks coming from the entities that have the ability to launch cyber-attacks or to support financially the cyber-pirates networks and make a fast intervention to cut their access to the Internet, in the context of one of the biggest fears faced by modern world, "cyberterrorism".

The concern for cyberterrorism have been seen at the level of both structures (NATO and EU) as well as at the level of each member state. For the North Atlantic Alliance, protecting its systems and communications has always been one of its priorities. For the first time, this function has been entered on the political agenda at the NATO summit in Prague in 2002, and came into the spotlight after the terrorist cyber attacks which have taken place in the year 2007 on public and private institutions in Estonia, a member of NATO.

[5] *Intelligence Magazine*, number 19, march – may 2011, pg.3;

At the European Union level, combating and preventing terrorism falls under the European Network and Information Security Agency, set up in 2004, which, in addition, manages preparatory technical activities for updating and developing Community legislation in the field of security of networks and information.

All these events have represented the alarm signal that led the authorities to adopting, in May 2013, the National Strategy for Cyber Security, which serves to identify vulnerabilities and risk factors on national critical infrastructures, the mechanisms of knowledge, preventing and combating terrorist threats, as well as authorized institutions to meet these challenges.

Although legislative measures subject to discussions and adoption, both at the level of each member state as well as higher level are aimed at protecting critical infrastructures and on the basis of the information in the case of cyber-attacks, deferred these initiatives considering that measures hinder freedom of expression, extending policies to online censorship damaging the impact and significance of information flow and affecting collective consciousness.

Their arguments are varied and reflect the idea that the threat is exaggerated "rarely is that critical infrastructure to be connected directly to the public network Internet"[6] ; systems in the private sector are far from being free of defense, and the "nightmare stories about their vulnerability are most of them apocryphal"[7], being an initiative aimed to justify offensive actions of military structures in the cyberspace and to attract more financial resources. In spite of these vicious remarks, the risk that tampered IT systems of economic entities, financial or public service of a member state is one not only real, but also achievable, and preventive actions are not only necessary but also imperative.[8]

## Conclusions

State entities, as well as individuals, are in a uncertainty, directly proportional to their own freedom. State actors will untertake more aggressive cyber attacks, with devastating effects, which will try to assign to non-state actors (organized crime, hackers, etc. )

It reveals an asymmetric situation with regard to actors involved in cyberwar. The attacks in this space are much cheaper, and produce severe effects , as compared to the conventional ones. The value of investments made in securing critical infrastructures is, unfortunately, inversely proportional to the size of effects caused by a potential attack against them. If it is desired to have a high level of security, then we need to take into account certain investments. Although in the last few years there have been budgetary adjustment, the cyberwarfare market is yet increasing.

A major effect of technological development makes actors the opportunity to migrate from a so-called blind-attacks, in which they were attacking multiple targets, hoping that they will get some results, to targheted attacks, where the victim is attacked directly and in force.

An aspect that should not be neglected is the fact that in August 2013, the president of Russia signed the national cyber security plan up to 2020, in which reference is made about the setting up of new special intervention troops, the so-called *"cyber-special troops"*.

[6] www.huffingtonpost.com, *Bianca Bosker*, Internet „kill switch", accessed on sept. 2013;

[7] www.executivegov.com, *Camille Tutti*, accessed on sept. 2013;

[8] *Intelligence Magazine*, number 19, march – may 2011, pg.3;

## References:

[1] T.Amza, C. Amza, *Criminalitatea informatică*, Ed. Lumina Lex, București, 2003;
[2] D. Denning, *Activism, Hacktivism, Cyberterrorism*
[3] Intelligence Magazine, *number 19, march – may 2011*
[4] NATO Magazine – *Noi amenințări, dimensiunea cibernetică,* http://www.nato.int/docu /review/2011/11-september/Cyber-threads/RO /index.htm, accessed in 05.09.2013;
[5] www.huffingtonpost.com, *Bianca Bosker*, Internet „kill switch", accessed on sept. 2013;
[6] www.executivegov.com, *Camille Tutti*, accessed on sept. 2013;