CYBER THREATS TO NATIONAL SECURITY. SPECIFIC FEATURES AND ACTORS INVOLVED

Anca DINICU
anca_dinicu@yahoo.com

"NICOLAE BĂLCESCU" LAND FORCES ACADEMY, SIBIU, ROMANIA

ABSTRACT

Security is not something given for sure, nor easy to obtain, especially in the current era of globalization, when actors present in the international environment have become much more diversified and the security threats seem to continually reinvent themselves. The current security environment is under the influence of some threats called "asymmetric", which defines new and extraordinary challenging circumstances the state has to face, by annihilating their effectiveness. The threat generated by a possible cyber attack or the cyber attack understood as a manifestation of threat exploiting a vulnerability is a matter of first rate when the national security strategy is set up and implemented. We are facing a new area of action – the cyberspace – to which we are more and more dependent due to the facilities it offers in order to achieve the national or strictly personal interests, but which also entails risks to the security of systems and networks on which we rely on to achieve objectives.

This paper aims to address the issue of cyber threats in terms of their features, but also to put in discussion the place and role of the State in the new battleground, the cyberspace.

Keywords

Security; state; cyber threat; cyber attack

1. The current international environment

The security environment, whether national or international, is characterized by constant change and unprecedented complexity. Everything happens very quickly, the normal aspects of the daily existence suddenly become very challenging, the yesterday's unconventional is today's traditional, the national interest is designed by taking into account the international interdependences, the global threats are hallmarked by a custom profile, being tailored by the effects they generate upon every society's wellbeing and by the degree of each state's functionality. We live in a world that hangs in balance between continuity and change, tradition and innovation, stability and uncertainty. Abstracting, it could be said that the symbol of the world at the still the beginning of the XXI century is Taijitu which brings together, under the circle's perfection and harmony, at least in terms of graphics, the Night (Yin) and the Day (Yang), respectively the evil forces, of seclusion and absurd, on the one hand, and on the other

hand, the forces of good, of harmony and coexistence.

The changing nature of the current security environment, as well as its complexity can be explained through a variety of arguments, including those that refer to threats more or less prominent, which generate risk to security by exploiting weaknesses.

The dynamism, complexity, and relative unpredictability of the direction to which the world is heading of are features of the international security environment, their existence and action becoming "natural" given the following facts:

• Global power structure is incompletely defined and the relations between the great powers are only apparently stable;

• Reminiscences of a thinking rooted in the Cold War logic;

• Weak governments unable to manage vulnerabilities not only by developing coherent policies based only on eliminating the effects, but also by issuing policies aimed on identifying and solving the causes;

• Disastrous discrepancy concerning development not only among states, but also within these or between classes and social groups;

• Emergence of radical ideologies that turn out to have a dramatic penetrating power upon individual or collective thinking systems;

• Inequitable access to resources, especially to the strategic ones;

• Terrorism and organized crime which, in comparison with the cyber attacks, could be considered from now as part of the older generation of asymmetric threats.

2. Characteristics of cyber threat/ attack

Nowadays, the cyber threat is one of the newest and most challenging threats to security, being able to jeopardize not only the safety of a state entity, but also the functioning of the international organizations, of the economic and financial companies. In the same time, the individual also could be the target of such attacks, if we take into cconsideration the growing digitization of payments and services and greater use of the internet for communication purposes. The wide range of possible targets envisaged by a cyber attack proves once again that security must be understood and be promoted in a multidimensional manner, as a result of the profound interdependence between the elements of the global social system and of the variety of the actors that can bolster or challenge the system's safety status. Thus, the "*cyber security embraces both the public and the private sector and spans a broad range of issues related to national security, whether through terrorism, crime or industrial espionage*" [1]. And if the intended target could be one of the mentioned subjects, when it comes to identify the perpetrator, this could be a hostile government/state, but also a non-state actor, like a cyber crime group or an extremist terrorist organization, which use cyber attack as a means of achieving political, economic or military goals.

The two types of actors come together on a battlefield called cyberspace, the consequences of confrontation, although extremely real, not being visible to the general public due to the fact that they are not reflected in images with great emotional impact on individuals, like in the case of a terrorist attack. Thus, for the ordinary citizen accustomed to perceive security first of all in terms of personal safety, is one thing to hear some news about a cyber attack launched in order to obtain information about one country's defense system or natural resources, and quite another to see how a plane flies into a sky-scraper.

The cyber threat is a threat to information technologies, i.e. technologies that allow the access, the exchange, and the transaction of information [2].

The cyber threat has features specific to the category to which it belongs, namely the asymmetric threats, but it also presents its own features that differentiate it from the others belonging to the mentioned category.

Just like the other asymmetric threats, the cyber one is also characterized by an obvious disproportion between those who launch the attack (usually few in number, putting at stake little resources, the action itself involving very low costs) and those over whom the attack is launched (which through the effects it generates can destabilize systems of national security or endanger businesses build at large scale). But in those cases when the cyber attack is decided at the government level, by extension, it can be presumed that an attack of a nation over another is planned and carried on. There are examples that can be brought in supporting this assertion, even though it is generally considered that "it is nearly impossible to know whether or not an attack is government-sponsored because of the difficulty in tracking true identities in cyberspace"[3]:

• Weeks before Russia invaded Georgia, in 2008, July 20, attacks had been already launched with the help of the „zombie" computers [4], the servers of the most important institutions in Georgia being blocked. This was not the first cyber attack made by Russia, who acted in the same manner against Estonia in 2007, „but it was the first time that an internet attack paralleled one on land" [5];

• Romania was also the subject of some cyber attacks conducted against institutions with special tasks conerning the state functioning, fact that entitled the Romanian Intelligence Service, as the national "CyberIntelligence" authority, to classify them as part of cyber assault category most likely carried out by state actors, without excluding other non-state potential attackers [6].

So, at least in the first instance, cyber attacks are characterized by anonymity, the cybercriminals being in advantage [7]. Having the possibility of assuming an almost perfect anonymity, these attacks can be launched from any of the nearly 2 billion computers existing all over the world, the number of internet connected devices reaching 8.7 billion in 2012 [8].

The threat coming from the cyberspace is implemented through some extremely various methods, such as [9]: socially engineered trojans and network-traveling worms; phishing attacks [10]; compromising confidential information by physical theft or loss; rogueware [11]; spam, targeted attacks,, identity theft; information leakage; search engine manipulation; or fake digital certificates. Therefore, this type of threat/attack is becoming more and more "sophisticated" because it requires a special skill set [12]. The actual costs concerning the undertaking of a cyber attack are not large, only some highly trained performers, able to identify security breaches of the network or system also based on sophisticated technology being required. These methods, by themselves and by their continuous improvement, are those which determine not only the sophistication mark of this type of attack, but in the same time its novelty. This case of confrontation is also characterized by the presence of two fighters (with the attacker unknown but often presumed), who are parts to a conflict based on political, economic and military goals and built on the most diverse attitudes and perceptions. So, the novelty refers to the means and methods by which the attack is done, the fight being carried on with the help of the cyber munition, which in no way replaces the conventional or nuclear one but only "enriches" the conflict architecture of XXI century.

3. The State on the map of cyber threats/ attacks

The cyberspace has adapted very well to the post-Cold War security environment, being also characterized by diversity when it comes to those gravitating in the new battle field. Thus, the cyber game is played by:

• Democratic or less democratic states, having very well defined interests concerning maintaining, regaining or conquering the power at the international level;

• International organizations which pay attention to the danger represented by the

cyber threat and develope strategies of preventing this type of threat;

• Multinational corporations and financial institutions that can be, because of the cyber attacks, exposed to some processes of economic espionage, intellectual property theft or discreditation in relationship with their stakeholders;

• Extremist terrorist organizations having political, economic and military special interests;

• Criminal groups and individuals known as "hackers".

There is general consensus that, up to present, the most dangerous actors in the cyber field are the nation-states (just as the state remains the main actor on the "real" international environment), the non-state actors, despite the performing technology they manage to possess, do not have the capabilities, determination and cost-benefit rationale of a nation state [13]. Probably the states interested in maintaining or conquering the international power and part in a fierce competition with other states that have or aim at same status are well equipped to launch targeted cyber attacks [14].

There are states that are daily subject to hundreds of cyber attacks. Usually, these are developed countries, having global interests and acting, due to their potential, as real powers. Regarding the sources of the attack targeting a state actor, these can be known/presumed or unknown adversaries, acting intentional as well as randomly choosing their targets, solitary hackers coming from inside or outside the country, or more or less friendly states [15], [16].

At least for the time being, "know your enemy" [17] is, for the targeted states turned into cyber attack receivers, rather a desire than a real thing. This does not mean the lack of effort in identifying the attackers and the lack of interest in issuing and implementing specific policies meant to mitigate the effects generated by the cyber attacks.

The cyber attacks are a serious threat to the national security and concern every aspect of our modern existence. The cyberspace manages the safety of the state and that of the people precisely by ensuring communication within the country (between state institutions, and between these and their constituents), facilitating international connections and being the virtual gateway of the very real goods and services.

According to various statistics, countries occupying the first ranks in the hierarchy of states from territory of which the cyber attacks are launched, without such action being necessarily sponsored by the state are: the Russian Federation, the United States and China, but also Germany, the United Kingdom, Brazil, Hungary, Turkey and Taiwan. [18], [19], [20]. Paradoxically, Romania founds itself in the forefront of the countries labeled as source [21]. Romanian cyber security experts argue that, most often, these attacks are actually done by cyber criminals from other states by using computers located in Romania which they infect and then turn them into "zombie", the cases when the perpetrator uses his private IP address in carrying out such actions being very rare. And this duality of identity may be an argument of an idea for more than 2,500 years old according to which "the whole art of warfare is based on deception" [22].

4. Conclusions

Worrying by the effects it generates and surprising by its spatial and temporal uncertainty of occurrence, the cyber attack is the "Achilles heel" of the modern state security, highly technologized and well developed, whose main problem is, in this matter, the proper and precise identification of the source. And the problem becomes more complicated as the attack is becoming more sophisticated.

References

1. http://www.cpni.gov.uk/threats/other-threats/
2. Neculae Năbârjoiu, *Securitatea informaţiilor*, (Bucharest: Editura Agir, 2008), 7.
3. http://online.wsj.com/news/articles/SB123914805204099085?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB123914805204099085.html
4. Computers taken over by a hacker without the knowledge of the owner, and connected to the internet.
5. http://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111
6. https://www.sri.ro/sri-confirma-investigarea-unor-atacuri-cibernetice-de-natura-sa-afecteze-securitatea-nationala-a-romaniei.html
7. http://www.enisa.europa.eu/
8. http://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/
9. http://www.cert-ro.eu/files/doc/789_20131114101107065907800_X.pdf
10. An attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.
11. A standalone malware computer program that pretends to be a well-known program.
12. http://www.usatoday.com/story/money/business/2014/08/28/jpmorgan-chase-bank-hack/14730183/
13. http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/RO/index.htm
14. Attacks adressed to a specific user, in order to have access to critical data in a hidden way.
15. http://asymmetricthreat.net/docs/asymmetric_threat_4_paper.pdf
16. https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions
17. Sun Tzî, *Arta războiului*, (Bucharest: Editura Militară, 1976), 41.
18. http://www.sicherheitstacho.eu/
19. http://www.wired.co.uk/news/archive/2013-04/24/akamai-state-of-the-internet
20. http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/
21. http://www.sicherheitstacho.eu/
22. Sun Tzî, *cit.ed*, p. 33.