STUDY REGARDING THE CYBER THREATS TO THE NATIONAL SECURITY

George-Daniel BOBRIC
dbobric08@gmail.com

"CAROL I" NATIONAL UNIVERSITY OF DEFENCE, BUCHAREST, ROMANIA

ABSTRACT

The virtual world became the ubiquitous background for daily interactions between individuals. The egregious interconnection of the last-generations devices is, in these latter days, an uncontestable reality. Despite the benefits provided by the interconnected world, there are unruly individuals, with a random savvy in the cyber domain, that furtively use it as their own asset. These actions are not performed wantonly, but having different substrates, from financial to political ones but, regardless the scope or the motive behind the ill-intentioned actions, cyber-attacks often lead to cascade effects to individuals, in particular, and organizations or even states, generally. Starting from this idea, in this paper is being assayed the way in which the cyber-attacks can be regarded as a major threat to the Romania's national security.

KEYWORDS:

Cyber-attack, cyberspace, national security, operational domain

1. Introduction

Nowadays, the world is facing a major change in the global geopolitical scene, with more and more actors developing new means and methods to impose their political vision among others or to fulfill their personal goals. Also, the progress made in the technological sphere, especially in the communication and information technology, open a door for some new state or non-state actors to misuse them in order to perform actions directed to cause harm for the victims.

In a report released by the Romanian National Computer Security Incident Response Team (2018), it is concluded that the cyber-attacks had a global character, being performed by actors from the entire world, with an overwhelming majority being effectuated from China (almost 63 percent). Starting from this idea, the overall objective of this article is to perform an analytical approach to the cyber threats to the Romanian national security, identifying the main actors which are involved in cyber-attacks, the reasons for performing them and the main effects that usually occur.

The actuality of the theme is given by the following aspects: the continuous development of the cyber domain, the evolution of cyber means and methods of exploiting the vulnerabilities from the cyberspace, the European trend of initiating new regulations and laws regarding cyberspace and improving the existing ones and, nonetheless, the need for identifying

DOI: 10.2478/bsaft-2020-0003

the risks from the cyberspace in order to ensure the cyber security and, moreover, national security at its core.

2. Actors involved in the proliferation of the cyber attacks

The main threat agents in cyberspace can be described as entities performing hostile activities in their own favor, in order to gain personal physical or psychical gains, such as cyber-criminals, insiders, nation-states, corporations, hacktivists and terrorists.

Cyber-criminals are individuals responsible for the majority of attacks worldwide nowadays, their main reason consisting of financial gains achieved from performing activities such as stealing or extortion. There is a close link between the organized crime and the informational crime, the last one being composed by cyber-attacks against people or financial sector, informational frauds – like illicit auctions or compromising the user's bank accounts on electronic commerce sites, and frauds using credit cards, by compromising ATMs and stealing sensitive data from the users' cards. In the specialty literature (McGuire, 2012), there are six types of cyber-criminals: swarms – organizations having a common purpose, but without a certain chain of command, hubs – individuals organized, with a common purpose and central command structure, with strong interactions between the members, hierarchies – traditional crime organization which extended their area of operations on the digital field (pornography, gambling), aggregates – temporary gathered members, without a clear purpose and strong interactions between them, and clustered / extended hybrid type – with members operating both online and offline (thus giving them the hybrid character), the difference between these two types being the existence/the lack of the central chain of command.

In the process of determining the origin of the cyber-attacks, a special attention is given to the sources located outside the organization. But there are also attacks done by individuals called insiders, which can also be extremely harmful. There are two types of insider attacks: deliberate or accidental. The first category can be also divided into two subcategories: planned or unplanned. Planned insider attacks are those types of attacks when an ill-intentioned person plans, in advance, to cause harm to an organization, involving joining it in order to cause harm from the inside. Unplanned insider attacks occur when an employee turns himself against the central point of view of the organization he belongs to and uses all means an methods to perform attacks in cyberspace from the inside networks he is connected to. Lastly, accidental insider attacks happen when a member of an organization does unintended harm to the company, for example, by accessing a malicious web site from where viruses are downloaded automatically.

As it can be noticed from the above, the insider attacks can be, very often, more dangerous and hard to anticipate than the external ones, due to the fact that the assailant already has access in the targeted zone, and he can furtively steal sensitive information from the inside (like server's IPs, internal networks configurations, passwords) which can be used lately from the exterior to jeopardize the organization's security. Moreover, an employee can also be aware of the vulnerabilities which exist within a company's network and exploit them for their own needs by cyber attacking the organization's cyber infrastructure.

Nation-states are the most important cyber actors, due to the fact that the ranges of means and methods that can be used in order to achieve some political or geostrategic goals are broad, with a myriad of actions done with the purpose of destabilizing the targeted organizations or even countries. More and more countries are trying to increase their cyber capabilities: if nowadays are only five recognized nuclear-weapons states (The United States of America, The Russian Federation,

France, China, The United Kingdom) and three declaring possession of nuclear powers (Pakistan, India and North Korea), dozens of countries are trying to improve their cyber offensive capabilities (Mills, 2017). Another reason for why nations states are considered to be important players on the cyber scene is the aim of performing this type of attacks (if the cyber criminals are mostly doing this type of activities for financial gains, the nation-states have higher purposes like spying, sustaining physical warfare with cyber-attacks, produce uncertainty and determining destabilization in other countries etc.).

The cyber-attacks executed by the nation-states or government-backed organizations have the power of disrupting the normal way of living for other countries' inhabitants. For example, there can be listed some of the destructive cyber-attacks performed by the nation-states: the WannaCry campaign (believed to be performed by North Korea) – a worldwide cyber-attack which affected hundreds of thousands of computer systems, encrypting the files and asking between $300 and $1200 for decryption, NotPetya (believed to be performed by actors from the Russian Federation) – a cyber-attack disrupting the activities of different organizations from banks to nuclear facilities, Stuxnet (believed to be performed by the US National Security Agency and Israel) – a cyber-attack performed against the Iranian nuclear power facilities and Industroyer (believed to be performed by actors from the Russian Federation) – a cyber-attack directed against the Ukrainian power grid.

Hacktivist is the name of those individuals who act in response to an issue of national or international concern. They can also be divided into other subcategories, according to the motivation they have and their target. For example, an international group called Anonymous launched several actions in response to Russian actions in the Crimean Peninsula, having at their core nationalistic motives, or the attacks against the Motion Picture Association of America, which had, at the inception, social motives.

Cyber terrorists can be described as the politically motivated actors which direct actions in cyberspace that involve physical or psychological damage caused by the interference of a remote digital action against a system. In the current days, the most determined to conduct digital attacks group is Daesh: in the past few years, savvy Daesh fighters had great success in transmitting propaganda. As an example, a British foreign fighter, with a large knowledge of the hacking domain, Junaid Hussain, managed to convince individuals with pro-Daesh orientations to conduct attacks in the name of the terrorist group. In this sense, some of the most notorious cyber attacks are those that targeted some France websites in 2015 and the Twitter feeds of the U.S Central Command, performed after he fled from Great Britain to Syria (Gunaratna, 2017).

3. The main reasons behind the inception of cyber-attacks

There is no action which is realized wantonly, and there may be a lot of motives behind evil-minded cyber actions, from those performed in order to demonstrate the ability to disrupt the normal activity of a certain individual or organization up to attacks performed by nation-states in order to achieve their political or geostrategic goals. If it is to look at the specialty literature, there are dozens of different motives listed by different authors. But many of them refer to and spin around four main dimensions: financial, cultural, social and political (Gandhi, 2011).

The financial gains are the main reasons for performing cyber-attacks. Attacks targeting the financial domain are effectuated in order to cause important financial loss to an individual or to an organization, to take out a "player" from the financial sector, to disable the possibility of settling transactions, to make people lose

trust in a specific institution or to request amounts of money in exchange for important data stolen by the attacker. Due to the fact that, nowadays, the resilience of institutions against cyber-attacks is questionable and the dependency on the online domain is increasing by day passing, related to the high connectivity between the financial infrastructure and the customers, a small cyber-attack can cause a cascade effect, which can lead to large-scale consequences.

In the last year, there have been a lot of cyber-attacks performed against the financial sector (Carnegie Endowment for International Peace, 2020). In February, the Metro Bank (based in the United Kingdom) was the victim of a new type of cyber-attack, which was intercepting text messages with specific credentials used to verify various transactions. In March, the Royal Bank of Scotland reported a cyber-attack that exploited a security flow, causing 50.000 computers to be affected. In May, an international cybercrime group, which used a malware called GozNym in order to steal over $100 million from over 40.000 victims, was deconstructed. In July, Capital One Financial Corporation was hacked by unknown individuals, thus causing a loss of 100 million person's personal and financial data, which have been published online. In September, it has been found out that hackers related to North Korea inserted malware in order to steal payment information from Indian financial institutions. It is believed that the attack was performed by the Lazarus group, which is known for developing cyber-attacks in order to finance North Korea's program of manufacturing weapons of mass destruction. Lastly, in November, Edenred (the global leader in payment solutions) reported that the company was the victim of a cyber-attack which caused damage to their organization's computers.

Also, there is another reason related to the financial zone. There are attacks performed by individuals in cyberspace in order to achieve money from the victims. Such attacks are done using the so-called "ransomware", which can be divided into two categories: encrypting and locker ransomware. The first type of malware is used in order to block the user's access to his personal files, which are encrypted, requiring payment for being able to access them again. The second type of malware locks the victims out of the operating system, with the targeted person not being able to access anything from the computer unless the operating system is changed.

The most recent and important ransomware attack is the one called "WannaCry", which is believed to have been performed in May 2017 by North Korean hackers. There were reported almost 200.000 computers across 150 countries to have been affected by the malware, which exploited a vulnerability found in the Microsoft Windows operating system machines, encrypted the files from the computer and asked payments in the Bitcoin cryptocurrency (in the amount of between $300 and $600) (Maxat, Vassilakis & Logothetis, 2019).

Another reason for performing cyber-attacks is the socio-cultural perspective. In the world, there are groups who share a specific set of beliefs. When one group tries to change the specific pattern which characterized it before, it may become the victim of another group. A very good example is the cyber-attack executed by Russian hackers against Estonia in 2007. This event was the result of an Estonian government's decision to relocate a monument from 1947, which was raised in the memory of Soviet troops who fought to gain control over Tallinn in the Second World War. The cultural view difference of the inhabitants over the event was extreme: while the Estonians saw the monument as a representation of the oppressing troops who killed their kinsfolks, the Russian population views the statue as the recall of the famous day of liberation. The removal of the monument began on the

27th of April, and the cyber-attacks campaign started the following day and lasted for three weeks (Gandhi, 2011).

The war between Israel and Palestine, which has, among others, cultural and religious motives, has been projected in the cyberspace also, especially in the last two decades. The cyber hostilities between the two countries begun in the 2000 year, when Israeli hackers attacked the Hezbollah's group (a Shia Islamist political party, a pro-Iran militant group from Lebanon) official website, inserting Israel's official flag and an audio file with the national anthem. Since then, the conflict increased in intensity, both in the physical and virtual environments. Israel's chief information officer (from that time) said that the war was taking place on three fronts: physical, the world of social networks and cyber (Roscini, 2014).

Last, but not least, another motive which stays at the base of the cyber-attacks is the political environment. In this case, attacks within the cyberspace can be done either internally (inside of a country, by extremist groups who protest against the ruling party, attack official websites, steal money in order to fund illegal activities like protests or riots, spread propaganda against their political enemies), or externally (by governmental organizations or state-sponsored groups who effectuate cyber-attacks against the country's enemy).

The first type of attack in cyberspace is not extremely harmful or dangerous, because the majority of the actors are not specialists in the cyber domain. But when it comes to the state-sponsored groups or organizations, the situation gets even more complicated. For example, in 2017, the world has faced an extremely virulent cyber-attack, which has been executed, according to the sources (McQuade, 2018), by the Russian hacking group Sandworm, although it has not been claimed by anyone up to now. The action has been done due to an update to the software which was installed on approximately 1 million computers from Ukraine. The company that sold the software was hijacked by hackers and, when the update was released, the piece of code was also released, causing an automatically and indiscriminately propagation of the malware. Also, in the previous year, a malware called Petya has been released in order to infiltrate in the computers from around the world and to force victims to pay for the decryption key; but NotPetya was designed only in a destructive scope, as the individuals targeted couldn't be able to gain access to their personal files even if they had paid the ransom. According to Ukrainian sources (Dearden, 2017), the malware affected several organizations from Ukraine, like Boryspil International Airport, Ukrtelecom, Ukrposhta, State Savings Bank of Ukraine, Ukrainian Railways. The attack also affected companies from outside of Ukraine, from hospitals in the United States to factories from Tasmania and Russia, where the state oil company Rosneft was hit.

This could be a very good example of a politically motivated cyber-attack, if the attack could be assigned to Russian hackers, as several officials have stated in the last years (Perez, 2016), and even if the consequences couldn't have been measured effectively by the originators, the main coincidence was that the attack occurred in the same day with the Ukrainian public holiday, the Constitution Day.

Nowadays, the world is facing a serious threat in the physical world: the pandemic caused by the SARS-CoV-2 virus. Also, the mal-intentioned actors noticed the negative effects this pandemic situation has on people and used different instruments to conduct cyber-attacks related to this disease. In the last two-three months, there have been recorded several cases of cyber operations performed by either APT groups or cyber criminals, using some of the instruments previously presented, the common aspect between them being the coronavirus theme. In this sense, a notorious case of this kind is the cyber

campaign launched, on March 2020, by a hacking group against the World Health Organization using a malicious website in order to steal the passwords of the organization's employees (Satter, Stubbs & Bing, 2020). So, even if the world faces a live-or-die situation, evil-minded cyber actors continue to profit from the cyberspace.

4. The effects of cyber attacks

Cyber-attacks have a plurality of effects, starting from the damage caused to different equipment and systems up to the reduction of the targeted organization's reputation. In the specialty literature (Agrafiotis, Nurse, Goldsmith, Creese & Upton, 2018), it has been written about 57 ways in which the cyber-attacks can cause harm to victims, individuals or organizations, which can be grouped in five major classes: effects on the machines, economic, psychological, reputational and, finally, societal ones. Starting from this point, we will analyze the impact of cyber-attacks on national security, taking into consideration the above-mentioned categories:

I. The targeted machine can be damaged either physically (for example, causing overheating of subcomponents) or digitally (by blocking the access to the operating system) or, even worse, completely damaged. This is the main concern for the critical infrastructure, which could be targeted in order to cause severe damage to different sectors (energetic, health, alimentation etc.). Also, the assets can be subjects to theft, thus being done either in the scope of gaining unauthorized, highly classified files, either in order to cause the malfunction of the system or to compromise it. The stolen documents can be further exposed to the public, as it has been done lately in a lot of cases by hacking groups (like Anonymous) or individuals. Moreover, another concern for the national security agencies, which has been increasingly seen in the last years, is the identity theft (like name, date of birth, email, physical address, telephone and bank account number, clinical information etc.), on one hand, and to personal information theft (for example, credentials that are stolen when approving online payments or transactions, digital signatures, etc.).

The most vulnerable organizations are those related to the government or the military: for example, an attack against the US Office of Personnel Management in 2015 conducted to more than 18 million federal employees' records being stolen, including job description and training details (Trend Micro, 2015).

II. Secondly, there are several economic consequences which are inflicted by the cyber-attacks. In the financial sector, the main problem may be the interruption of the operations realized either physically or online (payments, transactions, money exchange etc.). Related to this possible result is a cascade of aftermaths, including a reduction of the number of clients, due to the loss of trust, thus conducting to a decrease of the company's profit and, moreover, a decrease of growth of the company on the market. As stated previously in the article, there can also be some ransom payments required in order to regain access to important files. For the employees, these attacks can cause a loss of their jobs, and more financial losses for the company, as a result of the need to fulfill random compensation payments for the improper execution of the contract clauses. For national security, the impacts on the financial sector are a serious threat, causing a lot of damage in different domains with a chain of consequences that can also affect other sectors of activity.

III. Thirdly, the harmful effects of cyber-attacks can be seen in the psychological approach of the individuals. Even if the impact of the psychological harm done to individuals doesn't represent a very big threat to the national security, it can inflict a series of other consequences like frustration or anxiety for both managers

and employees, loss of self-confidence, sentiments of shame and guilty etc. However, the impact on national security can be increased by a series of crimes, suicide and deviant behaviors. For instance, in 2015, a group of hackers performed an attack on the AshleyMadison.com site (an online website used by people in order to find a partner for cheating) which, at that time, had almost 40 million users. The hackers were able to pilfer an amount of approximately 10 GB of users' personal data – name, physical and email addresses, phone numbers, the amount of money paid by the user for the services provided by the website. As a consequence of the attack, several cases of suicide have been reported by the police to have been realized in the background of the information released. Also, an increased number of divorces took place as a result of the hacking group's activity (Hopper, 2015).

IV. Fourthly, another important threat to the national security caused by cyber-attacks is the affected reputation of some organizations within the country or a decrease in the country's image on the international scene. A damaged perception of the public against the state's structures responsible for the security can cause a series of protests which can further lead to violent manifestations. Moreover, a damaged reputation can cause a loss of thrust, for organizations, from their customers or suppliers.

V. Last, but not least, is the impact that cyber-attacks have on society. As presented above, a loss of public trust in governmental authorities can lead to violent actions. Also, an important threat to national security is the obstruction of normal fulfillment of the state's functions or services. In December 2015, a major cyber-attack has been conducted by Russian hackers against three power plants from Ukraine, causing a major loss of energy, money and power outages for six hours, affecting nearly 225.000 persons. Subsequently, as this wasn't enough, the hackers also launched an attack against the telephony systems of the operator, thus leading to the inability to communicate with others (Whitehead, Owens, Gammel & Smith, 2017). As can be seen, this is a good example of how cyber-attacks can disrupt two important to people services: energetic and communications.

5. Conclusions

The cyber domain is the environment where different actors, with a multitude of points of view, needs and beliefs action in order to reach their objectives. These actors – from individuals to states – can have, like in the physic world, evil-minded behaviors, which often lead to the use of cyber instruments for performing virtual actions, of whose consequences are often threats to the national security.

The actors often have different motives, most of them being around four main categories: financial, cultural, social and political. Even if the individual performing the attack wants to gain money for his personal use, or has a cultural point of view different to the others and this leads him to cause harm, or even if the assailant has a personal problem with the ruling party from his country, the effects of these actions have, in the most cases, a cascade effect, affecting many other persons than the targeted victim.

To conclude with, cyber-attacks, regardless of their origin or motive, can represent a serious threat to international security, in general, and, particularly, to Romania's national security environment.

REFERENCES

Agrafiotis, A., Nurse, J., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity, Vol. 4, Issue 1.*

Carnegie Endowment for International Peace. (2020). *Timeline of Cyber Incidents Involving Financial Institutions*. Washington.

Dearden, L. (2017). Ukraine cyber attack: Chaos as national bank, state power provider and airport hit by hackers. *The Independent*, available at: https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html, accessed on 09 April 2020.

Gandhi, R. et al. (2011). Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine.*

Gunaratna, R. et al. (2017). *Cyber Terrorism: Assessment of the Threat to Insurance*. United Kingdom: Cambridge Centre for Risk Studies.

Hopper, T. (2015). Ashley Madison aftermath: Confessions, suicide reports and hot on the hacker's trail. *The National Post,* available at: https://nationalpost.com/news/canada/ashley-madison-aftermath-confessions-suicide-reports-and-hot-on-the-hackers-trail, accessed on 09 April 2020.

Maxat, A., Vassilakis, V.G., & Logothetis, M.D. (2019). WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms. *Journal of Telecommunications and Information Technology, Vol. 1, Issue 1*.

McGuire, M. (2012). *Organised Crime in the Digital Age*. London: John Grieve Centre for Policing and Security.

McQuade, M. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *The Wired Magazine*.

Mills, C. (2017). *Nuclear Weapons – Country Comparisons*. London: House of Commons Library.

Perez, E. (2016). U.S. official blames Russia for power grid attack in Ukraine. *CNN*, available at: https://edition.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/index.html, accessed on 07 May 2020.

Romanian National Computer Security Incident Response Team. (2018). *Threats evolution in the Romanian cyberspace 2018*. Bucharest.

Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press.

Satter, R., Stubbs, J., & Bing, C. (2020). Hackers tried to infiltrate the World Health Organization, the latest in a string of cyberattacks aimed at health officials during the coronavirus pandemic. *Reuters*, available at: https://www.businessinsider.com/world-health-organization-hack-tried-steal-passwords-with-fake-website-2020-3?r=US&IR=T, accessed on 12 April 2020.

Trend Micro. (2015). *US OPM Hack Exposes Data of 4 Million Federal Employees*, available at: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/us-opm-hack-exposes-data-of-4-million-federal-employees, accessed on 09 April 2020.

Whitehead, D. E, Owens, K., Gammel, D., & Smith, J. (2017). Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies. *70th Annual Conference for Protective Relay Engineers*, Washington.