CYBERNETIC ACTIONS ON CRITICAL INFRASTRUCTURES IN THE MILITARY FIELD

Maj. Petrișor PĂTRAȘCU, PhD Student*

The evolution, magnitude and effects of cyber attacks determined the states and organizations to undertake of increased security measures. Along with the development of new digital technologies, the number of Internet service users has considerably invcreased, which has also contributed to the unavoidable occurrence of ill -intended persons aiming to achieve a number of advantages through various illicit and controversial methods. Moreover, the profile of the cyber aggressor has advanced to the level of state and non-state actors. Thus, most of the targets that they identify as critical infrastructure belong to the military field.

Keywords: advanced persistent threat; cyber aggressors; critical infrastructure; APT28.

The importance and need for services provided by critical infrastructure in the society entails protection and resilience. The designation by states of the critical infrastructure at national level and the regulation of their protection have contributed to the inter-institutional dialogue, the coordination of protection from a central structure, the training of specialists in the field to jointly conduct simulation exercises by involving several institutions and government agencies in various sectors. In this respect, as a good example to those listed above, reference can be made to *the Critical Infrastructure Protection in Romania*, stemming from the legislative point of view from Emergency Ordinance no. 98/2010 on the identification, designation and protection of critical infrastructure, currently amended and completed by Law no 225/2018. Thus, by this law, vital functions are defined „*as those services that are essential to the functioning of society, such as: government business management, international activities; national defense; internal security; the functioning of the economy and infrastructure; security of population income and living standards*"[1].

Further on, by Law no. 225, the list of designated critical infrastructures has come to include 12 sectors and within the national security sector, one of the subsectors refers to country defense, public order and national security.

***"Carol I" National Defense University**
e-mail: *patrascupetrisor@yahoo.com*

Thus, each state institution which is found in one of the sectors mentioned in the law may be holding one or more critical infrastructure assets. Given the leading role of critical infrastructures in ensuring national security and their need to be protected, the access to critical infrastructure data and information is limited by the legislative requirements on the protection of both critical infrastructure and classified information which increases the interest of ill-intended persons or entities in obtaining and using as much classified information as possible. In this situation, cyberspace has become an environment conducive to such actions.

Profile of cyber aggressors

The diversity of cyber attacks has shown that there are several categories of actors, depending on their objectives. Therefore, according to *the Cyber Security Strategy of Romania*, the main actors that generate threats to cyberspace are: [2]

- persons or organized crime groups exploiting cyberspace vulnerabilities in order to obtain patrimonial or non-patrimonial advantages;
- terrorists or extremists who use the cyberspace to deploy and coordinate terrorist attacks, communication activities, propaganda, recruitment and training, fundraising, etc., in order to achieve their terrorist objectives;
- states or non-state actors who initiate or conduct operations in cyberspace in order to gather information from governmental, military, economic fields or materialization of other threats to national security.

Cyber threats are the product of these actors, often known as cyber aggressors or cyber attackers. Of the three categories listed above, the actions of states and non-state actors have the highest impact on national security, due to their resources, technological capabilities and time required, which underlie the preparation and launching of complex cyber attacks. In the terms of security of a state, in the light of the history of cyber-attacks, most of the actions of cyber-aggressors are directed towards national critical infrastructures, especially those of the energy sector, the financial and banking sector, and the defense, public safety and national security sector.

Terrorists or extremists use cyberspace for communication, information exchange, intelligence gathering, and unauthorized access to databases. The Internet has become a vast digital library that provides information about the targets, including some critical infrastructures, as well as anonymity in network digital communications.

The Internet represents both an active confrontation area for terrorist groups and a vital means of propaganda, communication, recruitment of new followers, exchange of experience and knowledge. In this context, the Internet has been used to create networks between terrorist groups, being an efficient way of rapid communication, enabling a decentralized organization that is difficult to be identified and monitored. [3]

Cybercriminals include people or groups of ill-intended persons who seek to gain financial advantages in a short time using various fraud schemes. According to McAfee's global 2018 study[4], the annual revenue from cybercrime has reached about $ 600 billion, representing 0,8% of global gross domestic product. In recent years, the increase in cybercrime has been influenced by both the use of new technologies by cyber criminals and the evolution of cryptomonas in cyberspace. At the same time, almost a quarter of the annual profit derived from cybercrime activities is intellectual property theft, and when military technology is threatened by cyber criminals, the national security is at risk.

Advanced persistent threats

Cyber actions directed toward critical infrastructure in the military field are conducted by state and non-state actors, and represent advanced persistent threats (*Advanced Persistent Threat – APT*). Advanced persistent threats are designed and launched by professional attackers on cyber infrastructures, backed by with the financial resources from some states or organizations. From the prespective of critical infrastructure in the military field, the main purpose of the persistent advanced threats is to obtain information at a high level of confidentiality, in order to have a strong impact on national security. Thus, there are precise objectives that are targeted by planning and launching attacks over a long period as long as they are not at risk to be found, which would compromise the information extraction.

Definitions of persistent advanced threats are quite varied, so one of them can be summarised by the meaning of the three terms as follows: [5]

Threats: APT attacks are not just codes and programs, and they are executed through coordinated actions of well-organized, funded, motivated and skilled people.

Persistent: The opponent has a well-established and prioritized mission, being guided by continuous monitoring and interaction by the organizing entity to achieve the final objective and to maintain the access to the target as long as possible.

Advanced: the opponent resorts to all the potential that he owns, including both intrusion techniques specific to computer systems and networks, and conventional techniques for gathering information such as telephone interceptions and satellite images. Along with available malware components, the opponents access and develop various tools, combining multiple targeting methodes and techniques.

From the perspective of Symantec specialists, advanced persistent threats are a type of targeted attacks (planned by targets) that use a variety of techniques. *The drive by downloads, SQL injection, malware, phishing, spam* are only a few of these techniques. A targeted attack is not necessarily an advanced persistent threat; however, this can always be said about APT. Therefore, below there are presented the ways in which advanced persistent threats differ from other types of targeted attacks: [6]

• *Customized attacks*: advanced persistent threats often use customized tools and intrusion techniques, adapted and developed specifically for a targeted objective. In this context we find exploiting zero-day vulnerabilities, viruses, worms

and rootkits programs. Another peculiarity is given by triggering multiple and chain threats to ensure permanent access to the targeted objectives. Sometimes a misleading threat is launched to give the impression that the attack was successfully repelled;

- *Low and slow actions:* they are framed over long periods of time by low and slow movements of the attackers, avoiding being detected as much as possible, until attackers meet their stated objectives;
- *Higher aspirations:* threats are designed to meet the requirements of international espionage and sabotage, which involved undercover state actors. The objectives of APT may be military, political or economic, and the groups behind APT are well-organized and funded, with the ability to operate with the support of military and state intelligence;
- *Specific objectives:* Compared to targeted attacks pursuing a larger spectrum of organizations possessing intellectual property or valuable information, APT targets a narrower set of objectives, including organizations that manage and exploit one or more critical infrastructures. In the military field, in addition to specific critical infrastructures, other entities, such as manufacturers and suppliers of military equipment and techniques, defense contractors or various partners are also targeted.

Overall, the diversified typology of cyber attacks highlights that any critical infrastructure owner in the military field may be targeted. Therefore, by their specifics, advanced persistent threats are planned to take advantage of the weakness of the security, not to be identified and to be effective as long as possible.

Notable APT attacks on critical infrastructures in the military field

The advanced persistent threats have moved from a commercial purpose to a strategic one, becoming instruments that can be exploited by many international players. The evolution of cyber attacks, including advanced persistent threats, lead to recognition of cyberspace as the fifth domain of operations by NATO. Thus, cyber security investments have increased significantly, advanced by adopting strategies in 2013-2014[7], continuing with the implementation of policies and procedures, the establishment of CERT teams, headquarters and cyber security governing structures, as well as the development and intensification of training, through multinational and inter-institutional involvement.

On the other hand, in response to all these measures, state and non-state actors have managed to develop sophisticated attack tools and techniques, planning and executing attacks on the most important targets. APT attacks carried out so far have had as main targets, in addition to critical infrastructure in the military field, other critical infrastructures in the field of security and defense. Many of the attacks, for security and confidentiality reasons, have not been made public.

The APT attacks listed in Table no. 1 represent some of the most representative attacks so far, targeting a number of entities with an important role in security and defense field.

In order to meet the targets, the attackers used various techniques, tactics and procedures. Of these, the most used techniques, tactics and procedures, highlighted in the previous table, have produced countless consequences for organizations, so they have to take increased cyber security measures.

Attackers have launched complex *spear phishing* campaigns on targets and the sent messages were containing topics specifically designed to draw people's attention in order to access malicious links containing malware. Spear phishing is a way sending messages to a group of users that share common items (they are employees of the same institutions, companies, departments, etc.). Emails are designed so that the recipient sees the sender as a known person (from whom he or she usually receives or waits for correspondence). Attachments containing malware have names that are similar to the recipient's domain[9].

The advanced persistent threat group APT28

Among the groups that have frequently launched APT attacks on critical infrastructures in military field from several states of the world, the APT28 threat group stands out, as being already established and very active in cyberspace.

The APT28, also known as Fancy Bear, Pawn Storm, Sednit, or Sofacy, has high status and high qualification among cyber attackers. In order to penetrate the target networks, the group used a diversified set of malware tools including: X-Tunnel, X-Agent and CompuTrace[10].

The attention on APT28 attacks can be described not only from the perspective of the large number of targeted objectives, but also from the perspective of the activity profile of these targets, most of them having the status of critical infrastructure.

In this context, one of the most prominent events in the aftermath of the APT28 attacks, which has gained international interest, is linked to the US presidential election campaign (2016), the main purpose of which is to influence the domestic policy of the country. [11]

Regarding the fact that APT28 threat group is targeting military targets or other important economic or technological targets connected to those referred to above, there is a constant interest in obtaining classified information as valuable as possible and seriously harming the national and international security and defense.

Below there are listed some APT28 actions on several military targets, suspected or confirmed by cyber security companies.

Actions directed against the Ministry of Defense in Montenegro. The security firms FireEye, Trend Micro and ESET have confirmed that Fancy Bear (APT28) has organized at least three separate attacks in January, February and June 2017, targeting several institutions in Montenegro. Using phishing specter tactics, the attackers wanted the intended users to open seemingly legitimate messages with relevant content about them, which allowed viruses to be installed on the computer. In January 2017, the Ministry of Defense of Montenegro was the target of an attack by several e-mails sent to wreak havoc. If messages were opened, Spear Phishing was automatically installed on victims' computers, along with APT28 malware. The next attack was February and lasted for several days, and the victims were government and state institutions websites, as well as the government-oriented media. The attacks were resumed in June 2017. Analyzing the diversity and purpose of these attacks, and the professional manner in which they were launched, the experts

Table no. 1

Notable ATP Attacks[8]

Denomination	Tehnigues, stratgies, procedures	Level of technology	Targetetd objectives
Red October	Spear phishing Social engineering Dropper Troian	Medium	Dimplomatic establishments Scientific research organizations
Cosmic Duke	Dropper Loaders Exploits Keylogger	Medium	Governmental institutions of NATO / EU member
Mini Duke	Social engineering Dropper Backdoor	High	Governmental institutions in the areas of foreign affairs, diplomacy, energy, telecommunications and defense
APT 28	Spear phishing Social engineering Wattering hole Backdoor	Highest	Governmental institutions in military and political fields NGOs, journalists and political parties of NATO / EU members
APT 29	Spear phishing Social engineering Backdoor	Highest	Governmental institutions Think-thanks, ONGs and media agencies
Turla	Social engineering Wattering hole 0-day	Highest	Embassies and consulates Governmental organizations in the field of foreign affairs

of the aforementioned companies confirmed that these attacks were synchronized. [12]

Actions directed against military targets in the Czech Republic. In 2017, several private Google email accounts of military personnel were compromised. Although the attackers did not get classified information, they were able to get more personal information and sensitive data. In addition, they also managed to compromise an IP address belonging to the Czech defense ministry by a malware known as X-Agent. The wave of spear phishing emails targeted mainly people from military diplomacy deployed in. Europe. The vector and targets of this attack fully correspond to the APT28 specific attack mode. Similarly, other spear phishing targeted European arms companies and a border guard of a European state. [13]

Actions directed against the Italian navy. Cyber security researchers from the Italian CSE Cybersec believe they have discovered an APT28 campaign targeting the Italian Navy in 2017, known as *„Operation Roman Holiday"*. They discovered a multi-stage campaign, initially based on the dropper malware program, written in Delphi programming language, followed by an X-Agent malware version downloaded from the Internet. Researchers have discovered an additional Windows DLL (Dynamic-Link Library) file that connect to a command-control server called "marina-info.net", similar to the Italian navy server, which made them believe it was developed to attack the Italian critical infrastructure protection and the other Italian cyber security institutions. [14]

Actions directed against Ukraine artillery. From late 2014 and through 2016, a malware (X-Agent) was distributed on Ukrainian military forums within a legitimate Android application, legitimately developed by a Ukrainian artillery officer. The application was developed to reduce the time it takes to fire by Ukrainian artillery units. The application has been used by over 9000 users. The ability of this malware was to retrieve communications and gross location data from an infected device in order to identify the general location of Ukrainian artillery forces and engage them. In the 2 years, open source reporting indicates that Ukrainian artillery forces have lost over 50% of their weapons. The peculiarity of these cyber actions is given by the expansion of APT28 application in mobile malware development. [15]

These examples are only a few events in the immense sphere of advanced persistent threats that targeted and damaged critical infrastructure and military personnel. The fact is that APT attacks already launched can be found in two hypostases. In the first hypostasis, it is important that some of these actions be known by the public while others have to become classified information. In the second hypostasis, there is an extremely dangerous situation for any cyber-infrastructure organization when persistent advanced threats are not discovered or are discovered very late, and many important data and information have been already exfiltrated.

Conclusion

The overflowing track of cyber-actions has determined states, international, national, public, and private organizations to take a number of cyber-security measures. Thus, the legislative regulations are largely identified in strategies and laws, models to describe cyber-attacks (e.g. Cyber Kill Chain, MITRE, Laliberte, etc.), security solutions offered by large companies and accredited by independent test laboratories, Incident Response Teams (CERT / CSIRT), cyber defense, command structures, and more.

In order to achieve effective protection against cyber-attacks, military organizations holding critical infrastructure, along with the rigorous application of technical security, should take into account people's vulnerabilities. Investing in promoting a solid security culture can be a viable, proactive and sustainable solution to reduce, as much as possible, the number and impact of cyber attacks.

NOTES:

1 Law no. 225/2018 for modifying and completing OUG no. 98/2010 regarding the identification, designation and protection of critical infrastructures.

2 Romanian Cyber-seucrity Strategyu, 2013.

3 C.F. Birta, *Cum este utilizat Internetul de teroriști*, accessed http://intelligence.sri.ro/cum-este-utilizat-internetul-de-teroristi, on 21.01.2019.

4 www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf, accessed on 18.01.2019.

5 http://www.worldinwar.eu/apt-advanced-persistent-threat, accessed on 26.01.2019.

6 https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf, accessed on 24.01.2019.

7 P. Pătrașcu, *The appearance and development of national cyber security strategies*, the 14th International Scientific Conference eLearning and Software for Education, Bucharest, 2018, p. 56.

8 https://www.sri.ro/categorii/publicatii, accessed at 22.01.2019.

9 M. Georgescu, Atacurile cibernetice de tip APT – noua dimensiune a spionajului, http://intelligence.sri.ro/ursul-chic-o-noua-dimensiune-spionajului, accessed at 28.01.2019.

10 https://www.ncsc.gov.uk/alerts/indicators-compromise-malware-used-apt28, accessed at 27.01.2019.

11 https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/st-senate-intel-committee-russia-election.pdf, accessed at 29.01.2019.

12 N.Popescu, S. Secrieru, *Hacks, leaks, and disruptions*, accessed on https://www.iss.europa.eu/sites/default/files/ EUISSFiles/CP_148.pdf, la 03.02.2019.

13 https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/en/ar2017en.pdf, accessed on 30.01.2019.

14 https://www.bluvector.io/threat-report-apt28s-operation-roman-holiday-attack-targets-italys-navy, accessed at 01.02.2019.

15 A. Meyers, *Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units*, https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units, accessed at 02.02.2019.

BIBLIOGRAPHY

Alexandrescu G, Boaru G., Alexandrescu C., *Sisteme informaţionale pentru management,* "Carol I" National Defense University Publishing House, Bucharest, 2012.

Bodmer S., Kilger M., Carpenter G., Jones J., *Reverse Deception, Organized Cyber Threat Counter-Exploitation*, The McGraw-Hill Companies, 2012.

Brenner S., *Cyberthreats: The Emerging Fault Lines of the Nation State*, New York, Oxford University Press, 2009.

Iorga I.M., *Securitatea informațiilor în acțiunile militare moderne*, "Carol I" National Defense University Publishing House, Bucharest, 2018.

Lucas G., *Ethics and cyber warfare: the quest for responsible security in the age of digital warefare*, New York, Oxford University Press, 2017.

Schmitt M., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd Edition. Prepared by the International Group of Experts at the invitation of NATO CCDCoE. Cambridge University Press, 2017.

Stallings W., *Cryptography and Network Security, Principles and Practice*, Fifth ed., Prentice Hall, 2011.

Turcu D., *Securitatea informațiilor*, "Carol I" National Defense University Publishing House, Bucharest, 2014.

Valeriano B., Maness R., *Cyber war versus cyber realities: cyber conflict in the international system*, New York, Oxford University Press, 2015.