DOI: 10.13166/WSGE/DYYC6119

Edit Bregu
WISDOM University College
edit.bregu@wisdom.edu.al

THE ISSUE OF CYBER-CRIME AS A MATTER OF NATIONAL SECURITY IN ALBANIA

ABSTRACT

The security challenges for Communication and Information Systems in Albania include all levels of the structures of the Ministry of Defense and the Armed Forces, starting from the individual equipment used in official working environments, to the provision of basic systems, which are critical to job performance. Some of the challenges that characterize this situation and their orientation for the future include: Th increasing threats in cyberspace, internet and mobile devices, social networks and portals, communication and transmission of information, creating a cybercrime market, espionage and sabotage, privacy and identity, anonymity and attributes, financial constraints, asymmetry of cyber warfare, etc. These will be some of the issues that this paper will try to address with reference to domestic and foreign literature, national and international legislation on cybercrime.

Keywords: *challenge, cybercrime, threat, legislation, internet, etc.*

Introduction

The Internet and new computer technologies have brought about colossal changes in the intercommunication of a global society. The transformation caused by this digitalization creates new dependencies. The economy, administration and provision of essential services now rely on the integrity of cyberspace and the infrastructure, systems and data that support it. The availability, integrity and sustainability of this infrastructure are constantly facing damaging actions[1].

[1] Singh S, (2002). The Code Book: The Secret History of Codes and Code-Breaking. Hapercollins.

Discovery has replaced defense as a strategy. Most of the hardware and software, originally developed to facilitate this environment, has prioritized efficiency, cost, and user convenience, but has not had a security designed from the beginning.[2] Malicious individuals, criminal or terrorist organizations may exploit vulnerabilities in liaison and communication systems, and minimizing these vulnerabilities is a national priority.

Bodypaper

Security challenges for Communication and Information Systems in Albania include all levels of the structures of the Ministry of Defense and the Armed Forces, starting from the individual equipment used in official working environments, to the provision of basic systems, which are critical to the smooth running of the work. Some of the challenges that characterize this situation and their orientation for the future include:

Rising threats in the cyberspace. Cyberspace, which anyone can use without time and geographical boundaries, asymmetrically gives advantages to malicious attackers, not to those being protected. As a result of sophisticated methods, the development of technological tools of cyber-attacks or the sponsorship of these attacks by states are serious, growing threats to national security. To prevent further aggravation of these threats, the creation of a "Free and Fair Cyberspace" must go hand in hand with the creation of a "Safe Cyberspace";

Internet and mobile devices. The development of the Internet and new computer systems, industrial control systems, mobile phones, mobile memory sticks and tablets, make us more efficient, but also more vulnerable in the environment where we exercise functional tasks;[3]

Social networks and portals: A particular challenge for open societies is the use of digital communication to influence public opinion, for example through covert attempts to influence discussions on social media and by manipulating information on news portals. This approach has already gained special importance as an element of hybrid warfare;

[2] Erickson J. (2008). Hacking: The Art of Exploitation, 2nd Edition Paperback. William Pollock Publisher.

[3] Singh, op. cit.

Communication and transmission of information: The network of the Ministry of Defense and the Armed Forces is not closed in a limited environment. Electronic communications with other structures of public administration, inside and outside the country, pose a challenge in itself due to conditions, mutual risk, different laws and regulations, which make it very difficult for the structures of the Ministry of Defense and Armed Forces to exercise control over them;

Creating a Cybercrime Marketplace: Developing an invisible, easily accessible marketplace for buying and selling information, as well as trading tools for cybercrime, has made it easier for criminals to take advantage of this ever-increasing opportunity, for benefits and malicious intent;

Espionage and sabotage: Military targets are and will increasingly be the target of attacks (hacking) and therefore espionage and sabotage make us more vulnerable to falling prey to electronic attacks on information and communication systems;

Privacy and identity: Personal privacy is also threatened due to new methods of communication and ways of using information systems and the Internet. Identity abuse is a growing challenge for every individual and institutional authority;

Anonymity and Attributes: Cyberspace has no physical boundaries. Cyberattackers are diverse, and the difficulty of identifying them makes their job easier (from individual hackers to organized crime groups to states), e.g. hackers and cybercriminals can take advantage of methods to launch attacks that are untraceable and difficult to eliminate;[4]

Cyber Warfare Asymmetry: In 300 milliseconds, a keyboard hit can travel twice around the world but, on the other hand, researchers can spend weeks, months to years identifying an attacker in cyberspace. Countermeasures are always overdue and hackers find vulnerabilities and exploit them to their advantage;

Financial constraints: Financial constraints are the biggest challenge possible. Considering that cyber security for many countries and organizations is a priority in concept and strategy, investments in "cyber security" need to be at the level corresponding to the actual risk;

But how can risk be managed?

[4] Ibid.

Threats

Cyber threats stem from the capabilities and efforts of an adversary to launch a cyber-attack on intelligence structures and military weapons systems, including sensors, navigation systems, naval surveillance, and airspace control.[5]

Based on the above, this category of attacks includes:

Sabotage: Cyber-attacks which disrupt the normal functioning of information structures

Espionage: Cyber-attacks which involve unknown interference by a third party to information structures to read, alter or add information.

Due to the rapid development of technology and areas of its use, in the future the defense will face objections which have cyber-attack and reconnaissance capabilities. These elements pose a real risk to the confidentiality and integrity of information, as well as to the availability of information structures, the Ministry of Defense and the Armed Forces, and other weapons systems (including sensors, naval surveillance navigation and space control air systems).

Weaknesses / violations

There is no complete security and protection in cyberspace. However, the possibility of a cyber-attack is many times greater than that of a physical attack. Experience has shown that various authorities and defense have been victims of cyber-attacks and, for the truth of this finding, will continue to face cyber-attacks in the future, but with limited success. As in the territory of our country and abroad in missions, defense personnel (Ministry of Defense and the Armed Forces) use the Internet (cloud computing), technological devices and mobile media (eg thumb drives, USB flash drives, etc.). The biggest challenge regarding their use is the awareness and warning of the staff who use them. Most cyber-attacks are caused by human error, so "internal threats" are real.[6] Critical information infrastructures of the Ministry of Defense and the Armed Forces are increasingly subject to complex cyber-attacks. Such

[5] Erickson, op. cit.
[6] Bazzell M, (2021). Extreme Privacy: What It Takes to Disappear Paperback.

attacks are carried out specifically against a specific target. For this reason, the Ministry of Defense and the Armed Forces form a "potential target" for terrorists or hackers who search for sensitive information. Due to the limited direct impact of cyber-attacks, the risk associated with them should never be underestimated.

The impact

An analysis of the threats and vulnerabilities will reveal the potential risk to which the impact and opportunity may be against the military defense environment. Therefore, a cyber-attack, which affects the availability, confidentiality or integrity of the Ministry of Defense and the Armed Forces, could have a major impact on the functioning of the institution, its structures and / or military operations…

1. Management and administration structures of the Ministry of Defense and the Armed Forces information structures will ensure that all Ministry of Defense and the Armed Forces personnel can work in a secure and protected cyberspace.
2. The development of military cyber defense capabilities in support of intelligence structures and actions of the Armed Forces will allow the strengthening of defense actions in information structures and operations, will also increase the security of operational networks and military systems against digital attacks.
3. In order to deal with problems arising from cyber threats, and to support Ministry of Defense and the Armed Forces structures, intelligence structures shall cooperate with internal and external actors, such as NATO, in accordance with the agreements of the signed…

Effects to be met:

a. keeping "cyber risk" at an acceptable level, to ensure the implementation of the military defense mission, through continuous analysis of cyber

threats, full management of cyber vulnerabilities and the possibilities of implementing cyber-attack detection and response tools tire;[7]

b. contributing to the storage and security of information to be able to carry out military missions successfully and fulfill legal obligations (guaranteeing the protection of classified and personal data);
c. defense in its entirety, must be able to protect genuine information structures and systems from cyber-attacks.

Taking into account the special nature of cyber security, the Ministry of Defense and the Armed Forces will continue to develop their capacities in this area according to the following priorities:

Priority I: A response system for cyber protection[8]. Rapid identification, information sharing, and rehabilitation can often reduce the damage caused by cyber-attacks. In order for these actions to be effective in the Ministry of Defense and the Armed Forces work environment, an interaction is required between the structures responsible for conducting analyzes, prior warnings to users, and coordinating joint efforts to minimize damage.[9] Ministry of Defense and the Armed Forces in order to be prepared to face a cyber-attack, which may take time until the normal working condition of the computer tools is restored, needs a disaster recovery plan from cyber-attacks. Liaison centers carry out surveillance and warning activities.

Priority II: Cyber Protection in the Ministry of Defense and the Armed Forces through the threat and vulnerability reduction program[10]. Violations of cyberspace also occur in critical Ministry of Defense and the Armed Forces infrastructure, including dependency structures, external support structures (such as Internet mechanisms), and insecure sites (locations) along the connection to computer networks. Weaknesses exist for a number of reasons, including technological weaknesses, poor security control during implementation and lack of detailed monitoring of the implementation of all necessary requirements for the security of the use of information structures.[11] A program

[7] Espinosa C, (2021). The Smartest Person in the Room: The Root Cause and New Solution for Cybersecurity. Lioncrest Publishing.
[8] Strategy about the cyber protection 2021-2023, Ministry of Defense, 2020.
[9] Bazell, op. cit.
[10] Strategy about the cyber protection 2021-2023, op. cit.
[11] Mitnick K, (2017). The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data. Hacette audio publisher.

to reduce cyber security threats and vulnerabilities will include coordinated joint efforts, which should be carried out by the responsible structures in the Ministry of Defense and the Armed Forces, in cooperation with other governmental and private sectors, to identify and rehabilitate serious cyber vulnerabilities and violations through collaborative activities. Exchange of best practices, evaluation and implementation of new technologies, components of the program which include raising awareness of cyber security.

Priority III: Threat assessment, documentation, their trend to increase understanding of the concept of cyber security.[12] The risk assessment will document the threats and their trend in relation to the Ministry of Defense and the Armed Forces information structures, as well as the impact on critical infrastructure and basic services. Their elaboration and description will be in such a way as to help increase the level of understanding of the situation and to show the threats and risks to the Information Technology systems.

Priority IV: Cyber Security / Protection Awareness and Training Program.[13] Many weaknesses in information systems are due to the lack of awareness on cyber security for the part of computer users, system administrators, procurement officers, systems audit staff, information security officers, security officers of information structures, etc,. These vulnerabilities may pose a serious risk to the systems, although they may not be part of the Information Technology infrastructure itself. Lack of trained staff further complicates the task of reducing vulnerabilities.[14] The joint cyber security awareness and training program will raise the level of awareness of staff and other structures in the Ministry of Defense and the Armed Forces. Capacities in cyberspace security will be developed in accordance with the modernization programs of information structures in the Ministry of Defense and the Armed Forces.

[12] Strategy about the cyber protection 2021-2023, op. cit.
[13] Strategy about the cyber protection 2021-2023, op. cit.
[14] Ibid.

Conclusions

There are institutional developments in terms of increasing cyber security or preventing cyber acts, but this is not enough. According to Mr. Kerluku, the former head of the Office Against Cybercrime in the State Police in Albania, there should be more proactive action, there should be more approach that we should not wait for it to happen, but we should be the ones who should find out, because this is not a crime that is obvious (Euronews Albania, 2020). The current trend shows that incidents will continue to increase, hence the cost of protection, as well as the effects caused by cyber-attacks will increase faster than the benefits that come from the basic services provided by information structures. But it is imperative to make significant improvements in increasing organizational capabilities versus cyber security requirements; providing a comprehensive approach to the structures of the Ministry of Defense and the Armed Forces, in order to have a clearer understanding of cyberspace and its weaknesses; need to increase the operational capacity of information structures in various aspects of cyber security; and staff awareness about cyber security needs to be raised.

References

Erickson J. (2008). *Hacking: The Art of Exploitation, 2nd Edition Paperback*. William Pollock Publisher.

Mitnick K, (2017). *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data. Hacette audio publisher.*

Singh S, (2002). *The Code Book: The Secret History of Codes and Code-Breaking. Hapercollins.*

Bazzell M, (2021). Extreme Privacy: What It Takes to Disappear Paperback.

Espinosa C, (2021). *The Smartest Person in the Room: The Root Cause and New Solution for Cybersecurity. Lioncrest Publishing.*

Strategy about the cyber protection 2021-2023, Ministry of Defense, 2020.

Strategy about the cyber protection 2018-2020, Ministry of Defense, 2017.

Strategy about the cyber protection 2004-2017, Ministry of Defense, 2003.

Key laws related to cyber security and crime

Law no. 7895, dated 27.01.1995 "Criminal Code of the Republic of Albania", i changed.

Law no. 2/2017 "On cyber security".

Law no. 9918, dated 19.05.2008 "On electronic communications in the Republic of Albania", amended.

Law no. 9887, dated 10.03.2008 "On the protection of personal data", as amended.

Law no. 8457, dated 11.02.1999 "On classified information", as amended.

Law no. 9880, dated 25.02.2008 "On electronic signature", as amended.

Law no. 107, dated 15.10.2015 "On electronic identification and services of trusted", amended.

Guide to good governance with cyber security. DCAF – Geneva Center for Security Sector Governance, Geneva – 2019.

Public-Private Partnerships in Cyberspace, ENISA, November 2017, https://www.enisa.europa.eu/publications/

public-private-partnerships-ppp-cooperative-models/at_download/fullReport

Public-private partnerships in national cyber-security strategies, https:// www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf

https://euronews.al/al/vendi/2020/01/18/siguria-kibernetike-shqiperia-mbetet-e-rrezikuar-nese-nuk-merren-masa/