Scientific Journal of Silesian University of Technology. Series Transport
Zeszyty Naukowe Politechniki Śląskiej. Seria Transport

Volume 107 **2020**

p-ISSN: 0209-3324

e-ISSN: 2450-1549

DOI: https://doi.org/10.20858/sjsutst.2020.107.13

Journal homepage: http://sjsutst.polsl.pl

Article citation information:
Ştefănescu, D.C., Papoi, A. New threats to the national security of states – cyber threat. *Scientific Journal of Silesian University of Technology. Series Transport*. 2020, **107**, 177-182. ISSN: 0209-3324. DOI: https://doi.org/10.20858/sjsutst.2020.107.13.

Daniel-Cornel ŞTEFĂNESCU[1], Alina PAPOI[2]

NEW THREATS TO THE NATIONAL SECURITY OF STATES – CYBER THREAT

Summary. Globalisation brought an electronic communications reliance, as well as some repercussions on the world's states, mainly in the sphere of cyber security. In recent years after the events in Ukraine, the cyber threat became a certainty and risk. We must be conscious that cyber attacks will grow up considerably, and one of their forms is the hybrid war, with its conventional and non-conventional, military and non-military capabilities. The emergence of a new battlefield – the cyberspace – is a reality, where military operations are carried out through sophisticated technology. For this purpose, states need to increase their cyber defence capabilities to prevent and combat aggression from the virtual environment to critical infrastructure, communications systems, and last but not least, the people.

Keywords: security, cyber attack, terrorist actions, communications system

1. INTRODUCTION

In the opinion of military analysts, there are four types of wars in history: first-generation wars (based on large human masses, for example, World War I), second-generation wars

[1] "Henri Coandă" Air Force Academy, Mihai Viteazul Street, no.160, Brasov, Romania.
Email: stefanesco_d@yahoo.com
[2] Romanian Defence Staff, Ministry of National Defense, Izvor Street, no. 110, Bucharest, Romania.
Email: alinagmr@yahoo.com

(based on great firepower, in which the development and use of armour and aircraft in battle had a decisive effect in the fate of the war, for example, World War II), third-generation wars (based on the principle of manoeuvre, supported by technological power and, implicitly, the speed provided by it), fourth-generation wars (corresponding to the age of information – their weapons are political, economic, social, cultural and military)[3].

The wars of the last generation do not fit into the classical, conventional forms of conflict resolution, and they unfold in a climate of insecurity, using its direct and indirect effects to "reach" the desired goals. This type of war eliminates the centre/centres of gravity, and not the human losses, especially among civilians[4].

The principles guiding the new war are informational predominance (the achievement of an informational supremacy capable of suppressing any action by surprise from a third party and ensuring a non-conflictual strategic environment), technological dominance, conflict symmetry (the parties involved in the conflict have similar means, policies, doctrines and strategies, dissymmetry (the tendency of each potential belligerent to achieve net superiority of forces, means, actions, policies and strategies that enable the achievement of supremacy with the least amount of losses and resources, policies, doctrines and similar strategies), and asymmetry[5].

2. NEW THREATS TO NATIONAL SECURITY OF STATES - CYBER THREAT

The end of the Cold War, in 1989, and especially the September 11, 2001 attacks on the United States demonstrated that the war had entered a new era in which the computer originally used to optimise office work gained offensive features.

After 1990, specialists in the field introduced a new term - "cybernetics", used to define a virtual physical space that people presented as actors behind the electronic activities of computer devices. Over the past 20 years, information technology has grown rapidly, cyber attacks by state or non-state actors have caused millions of dollars in damage, affecting a wide range of domains.

According to the Oxford Dictionary, cyber threat is "the possibility of a malicious attempt to damage or disrupt a computer network or system"[6]. The definition does not include the attempt to access different files, to infiltrate information devices or to steal data.

Nowadays, cybernetic treatment is used to describe information security issues. A cybernetic attack seeks digital devices through the cyberspace, a virtual space that does not exist.

The intention of the attacker is real, as well as the potential impact and outcome of the attack. While many cyber attacks are just unpleasant, some are pretty serious, even potentially threatening human life.

Cyber attacks can cause:

- interruption of water supply, natural gas, electricity,

[3] Nicolae Jingăroiu, *Războiul din generaţia a patra*, in *Forţele Terestre*, no. 1, 2009, Buletin de Teorie Militară, editat de Statul Major al Forţelor Terestre, available at http://www.revista.forter.ro/2009_1_t/02-tgl/04.htm

[4] Ovidiu Moşoiu, Raluca, Vasile, Adelina Petrovai, *Aspects of the EU security issue in the 21st century"*, Editura Academiei Forțelor Aeriene „Henri Coandă, Braşov, 2018

[5] Mihail Orzeaţă, *Are We Prepared for the War of the Future?,* Gândirea Militară Românească no.4 octombrie-decembrie 2016, Bucureşti, 2016

[6] Available at: https://en.oxforddictionaries.com/definition/cyberthreat

- disruption of the operation of telephony networks, public transport systems, navigation systems,
- disruption / delay / blocking of the operation of military and national security systems,
- modifying / deleting personal databases (personal data, accounts, medical records).

3. TYPES OF THREATS TO CYBER SECURITY

Attackers launching cyber-security threats target three broad categories of intentions, namely:

- creating disorder,
- financial gain,
- espionage (including the corporate one - patent theft and state espionage).

As for attack techniques, state or non-state actors as well as malicious actors, use a wide range of cyber threats:

- Malware – consisting of software that performs an intentional activity that targets a computer corruption or infiltration into a target network, for example, deleting / modifying data or taking control of a system.
  It causes:
    - blocking access to various key network components (ransomware),
    - installing harmful programs,
    - obtaining information by sending data from the hard drive (spyware),
    - disturbance of certain components, which makes the system inoperable,
- Phishing - consisting in carrying out an email attack on a possible target, which involves deceiving the recipient of the email to disclose confidential information or download malware by clicking on a hyperlink in the message,
- Spear Phishing – is an advanced form of phishing whereby the attacker studies the victim (individual, organisation, or business) and intentionally uses emails, messages, and other platforms to cause users to disclose personal information or perform actions that cause network compromises, loss of data or financial loss,
- “Man in the Middle” (MitM) attack – when an attacker establishes a "link" between the sender and recipient of electronic messages, intercepts them and changes their content. The sender and the recipient believe they communicate directly with each other.
  There are two common entry points for attacking:
    - through unsafe public Wi-Fi networks, attackers can "place" themselves between a visitor's device and a network so that the information is sent through the attacker,
    - after the malware is uploaded to a device, an attacker can use the software to process all the victim's information,
- Trojan – it is a type of malware that installs itself into a target system as regular software, but once installed, damages / blocks the "host" software,
- Ransomware – it consists of an attack involving data encryption in the target system, as well as the request for a ransom in exchange for allowing the user to access their own encrypted data,
- Denial of Service Attack or Distributed Denial of Service Attack (DDoS) – it occurs when an attacker takes command over multiple devices and uses them simultaneously, potentially interfering / overloading target systems,

- Attacks on IoT (Internet of Things) Devices – it consists of attacks afflicted by the Internet over individual IT / corporations / state institutions, which can be taken over by these systems,
- Data Breaches - a data breach is a security incident where information is accessed without authorisation. Data breaches may cause various deficiencies in the way businesses and consumers operate in a variety of ways. They generate a costly expense and require a long time to repair,
- Malware on Mobile Apps – Mobile devices as well as other computing devices are vulnerable to malware attacks. Attackers can "launch" malware into app downloads, mobile sites, phishing emails, and text messages. Once compromised, a mobile device can offer the attacker access to personal information, location data, financial accounts, and more.

Cyber threats are unlimited in number and ways of manifesting and can be generated from different places, by different people and in different contexts, as follows:

- various people who "produce" attack vectors using their own software tools and their own knowledge,
- criminal organisations, which either through their own employees or through third parties, develop attack vectors and attacks on possible targets in the area of interest,
- various organised crime groups,
- terrorists,
- industrial spies,
- national states that encourage "masked" cyber attacks,
- hackers,
- business competitors.

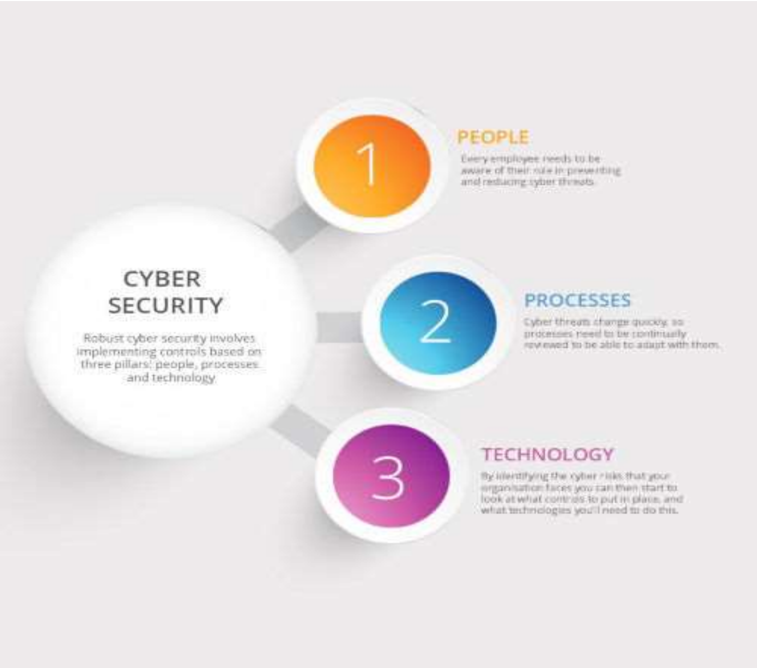
4. CYBER SECURITY

Cyber security focuses in particular on protecting information systems and their components – including hardware, software and data, as well as digital infrastructure from an attack, unauthorised access, damage or inaccessibility. Databases, websites, programs, servers, or accounts can be exploited through a cyber attack.

In recent years, cyber security has been subject to intense media coverage due to the rapid development of cyber-related risks, both in terms of size and number, and the degree of impact on individuals, governments and organisations.

The robustness of cyber security (and information security) involves the implementation of controls based on three pillars: people, processes and technology. This approach helps organisations protect themselves from both organised and opportunistic attacks as well as common internal threats.

Efficient cyber security uses risk management to ensure that these controls are implemented cost-effectively – in other words, based on the likelihood of risk and the worst possible impact if the risk materialises.



Robust cyber security involves implementing controls based on three pillars: people, processes and technology

Every employee needs to be aware of their role in preventing and reducing cyber threats.

Cyber threats change quickly, so processes need to be continually reviewed to be able to adapt with them.

By identifying the cyber risks that your organisation faces you can then start to look at what controls to put in place, and what technologies you'll need to do this.

Fig. 1. Cyber security[7]

5. CONCLUSIONS

Implementing effective cyber security measures is particularly challenging today, as there are more devices than people, and attackers are becoming more and more innovative.

The most effective strategy to mitigate and minimise the effects of a cyber attack is to build a solid foundation on which cyber security technology should be developed, with multiple layers of protection spread across computers, networks, programs, or data intended to be kept safe.

People, processes and technology need to complement each other in an organisation in order to create an effective defence against cyber threats.

References

1. Botha A., J.A. Badenhorst-Weiss. 2019. “Risk management in a bulk coal export logistic chain: a stakeholder perspective”. *Journal of Transport and Supply Chain Management* 13(A424): 1-16. DOI: https://doi.org/10.4102/jtscm.v13i0.424.
2. Carlini J. 2017. *Geneva Convention in Cyber warfare? Don't Count on It*. Available at: https://intpolicydigest.org/2017/08/06/geneva-convention-cyberwarfare-don-t-count/.
3. *Communications Security, Reliability and Interoperability Council.* 2017. Final Report - Cyber security Workforce Development Best Practices Recommendations. Available at: https://www.fcc.gov/files/csric5-wg7-finalreport031517.

[7] Available at https://www.itgovernance.co.uk/what-is-cybersecurity

4. Cortada James W. 2007. *The Digital Hand. Vol 3: How Computers Changed the Work of American Public Sector Industries*. USA: Oxford University Press. ISBN: 978-0-19-516586-9.
5. Hernandez P. 2016. *Commission on Enhancing National Cyber security*. Available at: https://www.nist.gov/cybercommission.
6. Hudakova M., J. Dvorsky. 2019. "Analysis of the Market Risk Sources in the Small and Medium-Sized Enterprises of Transport". *Communications - Scientific Letters of the University of Zilina (Komunikacie)* 21(4): 97-103.
7. IT overnance. Available at: https://www.itgovernance.co.uk/what-is-cybersecurity.
8. Jingăroiu Nicolae. 2009. "Războiul din generaţia a patra". [In Romanian: "The fourth generation war"]. *Forţele Terestre* 1. Buletin de Teorie Militară editat de Statul Major al Forţelor Terestre. Available at: http://www.revista.forter.ro/2009_1_t/02-tgl/04.htm.
9. Ovidiu Moşoiu, Raluca Vasile, Adelina Petrovai. 2018. *Aspects of the EU security issue in the 21st century*. Braşov: The Publishing House of the Air Force Academy "Henri Coandă".
10. Medić D., Z. Lušić, R. Bošnjak. 2019. "Comparative analysis of the maritime venture risk and the cost of averting a fatality in the Republic of Croatia". *Nase More* 66(226): 62-69.
11. Mihail Orzeaţă. 2016. „Are We Prepared for the War of the Future?" *Gândirea Militară Românească* 4.
12. Lewis James, Katrina Timlin. 2011. United States. Center for Strategic and International Studies. *Cybersecurity and cyberwarfare: preliminary assessment of national doctrine and organization.* Washington, D.C.
13. LEXICO. Available at: https://en.oxforddictionaries.com/definition/cyberthreat.
14. The Global Risks Report 2018. 13th Edition. *World Economic Forum.* Available at: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.
15. Simba S., W. Niemann, T. Kotzé, A. Agigi. 2018. "Supply chain risk management processes for resilience: a study of South African grocery manufacturers". *Journal of Transport and Supply Chain Management* 11(A325): 1-13. DOI: https://doi.org/10.4102/jtscm.v11i0.325.
16. Snell E. 2017. *Addressing the Cyber security Skills Gap with Improved Training*. Available at: https://healthitsecurity.com/news/addressing-the-cybersecurity-skills-gap-with-improved-training.
17. The Romanian parliament. Law no. 362/2018 on ensuring a high common level of security of computer networks and systems. January 2019.

Received 10.03.2020; accepted in revised form 20.05.2020