

**GRZEGORZ PILARSKI\***

Akademia Sztuki Wojennej, Warszawa, Polska

## CYBERSECURITY – CHOSEN ASPECTS

**ABSTRACT:** In the era of contemporary cyber threats, there is an urgent need to provide cybersecurity in almost every public institution as well as in business. Particular emphasis should be put on institutions which are responsible for ensuring national security. A specific case is a military organization where cybersecurity should be provided during peace, crisis and war. In this article the author presented selected problems related to providing cyber security in a military organization and proposed appropriate solutions to the indicated aspects.



**KEYWORDS:** cyberspace, cybersecurity, national security, Computer Emergency Response Team (CERT), information communication technology (ICT),

### INTRODUCTION

Nowadays, many people are fascinated with varied aspects pertaining to cybersecurity. Some of them would like to learn specific information for example how to hack Wi-Fi or other ICT systems. The others would like to know how to provide security of their data and systems in which the data is generated, processed, stored and transmitted. Providing cybersecurity is a complex process and it requires a constant supervision in the light of fast developing ICT branch. A set of tips how every individual user of cyberspace<sup>1</sup> can have influence on their own cybersecurity in the network is presented below on the list of 10 Internet Security Rules<sup>2</sup>:

---

\* **ptk dr hab. inż. Grzegorz Pilarski**, War Studies University, Warsaw, Poland

 <https://orcid.org/0000-0001-9728-2611>  [g.pilarski@akademia.mil.pl](mailto:g.pilarski@akademia.mil.pl)

Copyright (c) 2022 Grzegorz Pilarski. This work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.

<sup>1</sup> See G. Pilarski, *Tackling cyberspace threats – the international approach*, Security and Defence Quarterly, 2016, Volume 3, No. 12, pp. 104.

<sup>2</sup> See 10 Internet Security Rules. Retrieved October 2, 2022 from: <https://www.nortonlifelockpartner.com/security-center/10-computer-security-rules.html>.

1: Keep computer viruses and spyware out.

It is easy to say but it is important to remember that hundreds of new computer viruses are created every month. Every computer is vulnerable but the best way to stop viruses is to install antivirus software and update it regularly.

2: Block hackers and intruders with a firewall.

Hackers are everywhere in the web. In the author's opinion the article on the Internet security rules was probably read by some of them too, although nobody would admit it. A firewall separates your computer from the Internet and decides what gets in or out.

3: Be careful when opening emails and attachments.

Everyone gets hundreds of e-mails and some of them carry a virus, worm or "Trojan horse". We should not open e-mails from unknown sources, we should delete such an e-mail with attachments. Do you know what is cyber slacking? This is opening your private e-mail on devices at work and this way we infect the infrastructure. For example: do you know what it is ransomware? This is the activity of hackers or rather crackers to encrypt your data on your computer. One day at my work one lady had such a problem. She opened pdf attachment from e-mail which she thought it was an e-mail from printer-scanner so as a result she lost her data.

4: Be selective about what you download and from which sites.

Definitely, we should not download any files from suspected websites.

5: Choose a password that is better than "password", it has to be complex today.

We should choose password easy to remember but difficult for other people like hackers. Moreover, it is a good idea to change it from time to time but not later than after three months.

6: Do not let your web browser remember your personal information, turn such options off.

We have to know applications which we use especially Internet browser thus we should delete temporary files and do not save any passwords on our computer.

7: Protect your kids online, observe them and what they do on the Internet.

Of course if you have children now or in the future. It is very important to control the activity on the Internet because children are an easy prey.

8: Keep your private life private, you don't know people out there.

We should not save personal information concerning private data of our families on-line. We do not know who is on the other side.

9: Backup your computer, regularly, both data and OS configuration.

This point is very important and we have to remember that we can lose our data.

10: Update your Internet security software regularly, upgrade to new versions.

If we do not do this our computer will be vulnerable to cyberattacks.

Although, it might seem complicated, all these ten Internet safety and security rules are actually easy to follow and obey. By following them, in cyberspace<sup>3</sup> you will: protect your family and friends, save your personal and other valuable data, save your money, time and avoid frustration.

Let me recall the 9th point about backup. In the author's opinion the following sentence is true and very important: "there are only two types of computer data. Those that we have backed up and those that have not been lost yet."

As you see there are many factors which everybody who is interested in cybersecurity has to take into consideration. In the light of an urgent need to provide cybersecurity in almost every public institution as well as in business, the main research question posed by the author of this article is: How to ensure cybersecurity in a military hierarchical organization?

This case is specific because a military organization provides national security and ICT systems have special requirements connected with the protection of classified information. It does not change the fact that such an approach to cybersecurity that is used in a military organization can be successfully applied in other sectors of public life. The assumption that cybersecurity in a military hierarchical organization should be considered through the prism of legal factors, national and international regulations, organizational and technical security, depending on the character of an organization, constitutes a hypothesis which can be adopted here.

The author is aware of the fact that the field of research is very broad and the article presents only chosen issues in terms of cybersecurity.

---

<sup>3</sup> Cyberspace - in Poland the definition of cyberspace was presented in the amendment to the Act of 30th August 2011 on the state of war and the competencies of the Commander-in-chief and the rules governing his subordination to the constitutional bodies of the Republic of Poland. In accordance with the document cyberspace is defined as "a space of processing and exchanging information created by the ICT systems, as defined in Article 3 point 3 of the Act of 17 February 2005 on the informatization of entities performing public tasks (OJ No. 64, item 565, as amended), together with links between them and the relations with users; in accordance with Article 2 paragraph 1b of the Act of 29 August 2002 on martial law and the powers of the Supreme Commander of the Armed Forces as well as the Commander's subordination to the constitutional authorities of the Republic of Poland (OJ No. 156, item 1301, as amended), Article 2 paragraph 1a of the Act of 21 June 2002 on the state of emergency (OJ No. 113, item 985, as amended) and Article 3 paragraph 1 point 4 of the Act of 18 April 2002 on the state of natural disaster (OJ No. 62, item 558, as amended)".

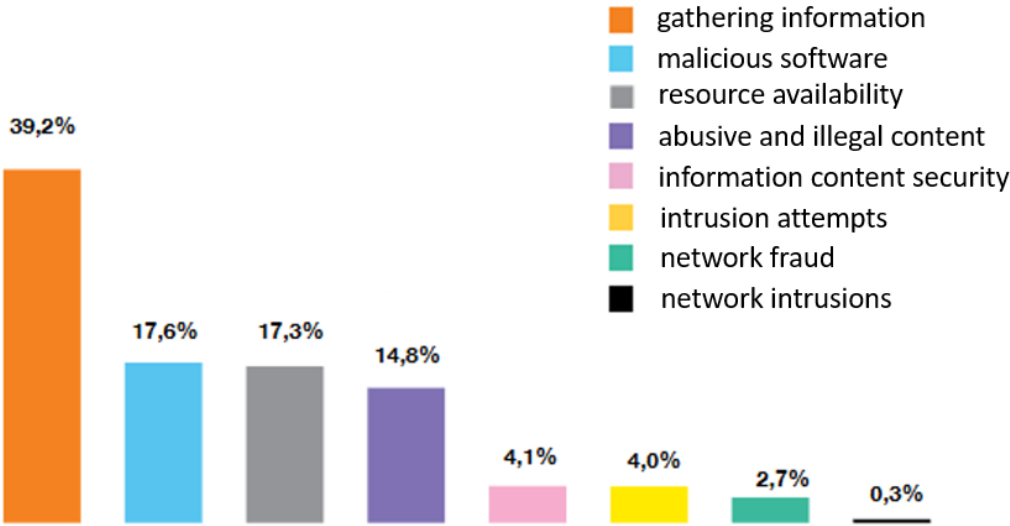
**NATIONAL AND INTERNATIONAL CONSIDERATIONS OF CYBERSECURITY**

At the beginning, we should ask ourselves a question “should we deal with cybersecurity?” Let’s look for answer. Taking into consideration some statistical data we can see that one of telecommunication providers noticed over 335 million phishing incidents blocked and near 5 million events related to malware<sup>4</sup> during a year. This is only a view on cybersecurity of one company for one month. Imagine how many such cases are in the whole country like Poland or around the world. It makes you think that we should get interested in this area.

Most of incidents concern gathering information but near 18 percent concern malicious software (see Fig. 1).

Fig. 1.

Characteristics of computer incidents in 2021 handled by CERT Orange Polska



Source: CERT Orange Polska Report CERT 2021, pp. 18-19.

Other source shows that cyberattacks are associated with the theft of money. Should we deal at all with such attacks? This is another reason that cybersecurity is an important issue. Is only the theft of money important? Perhaps more important is information stealing. However, interest in ransomware attacks has increased in recent years. The word ransomware is a combination of two words ransom and software. Ransomware is based on the fact that malicious software installed in the operating system blocks access to the system or prevents reading of saved data by using encryption techniques and then demands a ransom from a victim

<sup>4</sup> See CERT Orange Polska Report CERT 2021, pp. 5-29.

for the restoration of the original state. This practice is becoming more frequent today. We must remember and realize that cybercriminals do not know borders. Their activity in an international environment is not always possible to counteract because of the laws and rules of operation in various countries in which cybercrime takes place. So, how can we defend against cyber threats? Is it enough that we close ourselves within our own countries and create a high wall on the state border? The author, taking part in cybersecurity conferences, received the opinion that some states as big powers can do this and they will be safe. Such reasoning in today's world is unacceptable.

What about legal conditions on this aspect?

The basic legal act regulating the aspects of cyber activity is the directive of European Parliament and Council on the security of network and information system of the six of July 2016 called NIS in short. Under this directive the member states are obliged to create national system to monitor computer incidents through creating special teams called CERTs or CSIRTs as well as to identify the operators of core services. Due to the fact that threats in cyberspace are borderless, and taking into consideration article 13 of the Directive NIS in the scope of international cooperation and article 218 of the Treaty on the Functioning of the European Union in short TFEU the European Union has to establish international agreement with third countries or international organizations.

The same aspects were raised on the international governance forum under the auspices of United Nations in 2017. During workshops number 38 which main topic was international cooperation between CERTs, technical diplomacy and cybersecurity, the members indicated that international cooperation in this scope is on a low level requiring special attention at the time of contemporary cyber threats. Thus, in the world there are different subjects called into being such as CERT, CSIRT, IRT, CIRT or SERT which have similar tasks. Of course we must remember that the name CERT is a proprietary name limited only to the members of FIRST organization that is Forum of Incident Response and Security Teams<sup>5</sup>. FIRST brings together a lot of security and incident response teams including especially product security teams from the government commercial, and academic sectors. Poland has four teams like that. Moreover, in Poland we have many organizations dealing with cybersecurity issues.

---

<sup>5</sup> Forum of Incident Response and Security Teams was establish in 1989 in USA because of the infamous Internet worm (Morris Worm).

The name CERT is a proprietary name, thus a group alternative to CERT can be Computer Security Incident Response Team (CSIRT) as a team for computer security and response to incidents. The term CSIRT is mainly used in Europe instead of 'CERT', which is registered in the USA by CERT Coordination Centre (CERT/CC). To refer to the same type of teams the following varied names are used:

- Computer Emergency Response Team / Coordination Centre (CERT or CERT/CC );
- Computer Security Incident Response Team (CSIRT) team for computer security and response to incidents;
- Incident Response Team (IRT);
- Computer Incident Response Team (CIRT);
- Security Emergency Response Team (SERT) team for fast response to security threats.

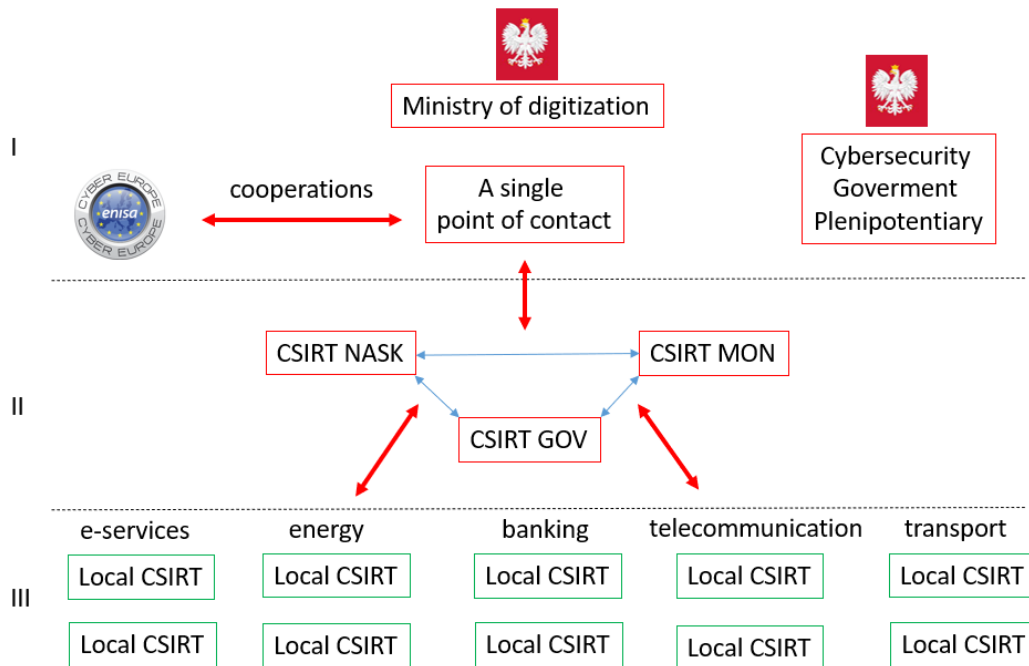
As it has been mentioned above, on the basis of the NIS directive the Ministry of Digitalization prepared the national system of cybersecurity of the Republic of Poland which had been accepted by the council of ministers and signed by President of RP<sup>6</sup>. The documents were the basis for preparing the structure of national computer incident response system (see Fig. 2).

---

<sup>6</sup> OJ No. 2018, item 1560 of 5th July 2018 on the national system of cybersecurity.

Fig. 2.

Structure of national computer incident response system



Source: Own elaboration based on the Act of 5 July 2018 on the national system of cybersecurity (OJ No. 2018, item 1560).

This scheme presents the structure of national computer incident response system. It is divided into three levels namely: the first one is strategic-political level, the next one is operational level and the last one is technical level. On the first level there is competent authority as Ministry of Digitization, Cybersecurity Government Plenipotentiary and A single point of contact. A single point of contact is responsible for cooperation between CSIRT teams of second level and EU CSIRT team. The operational level entails three main sectors CSIRTs such as: CSIRT GOV (government), CSIRT MON (military supplied by the Ministry of National Defense) and CSIRT NASK (national research institute supervised by the Ministry of Digitization). On the technical level there are CSIRTs created in given sectors like: critical infrastructure for example e-services, energy, banking, transport, telecommunication which are responsible for monitoring ICT networks. Nowadays, the presented system is being created and additional legal acts are under legislative process.

Next important issue is cybersecurity system of the Ministry of National Defence. The system is normalized on the basis of a decision number 396/NCBC of the Ministry of National

Defence of November 2019. The structure of cybersecurity system involves the following information bounds:

- dependency relations;
- cooperation in terms of ICT security;
- cooperation;
- cooperation with institutions from outside the Ministry of National Defence.

In the system we can notice cooperation in terms of ICT security which involves Military Police and the Military counter intelligence service. The next relation concerns dependency relations and here we have ICT systems organizers and the heads of national defence units.

The next relation is cooperation, it entails the whole system. The last relation is cooperation with institutions from outside the Ministry of National Defence. The most important in this scope is relation between NATO CSIRS Coordination Centre and NATO CSIRS Technical Centre.

As the author mentioned, there is one significant fact to remember i.e. cybercriminals do not know borders thus, we definitely need to join forces and develop international cooperation to combat cybercriminals. Moreover, international cooperation is not effective enough at this point thus, it is a must to cooperate on the international scene and change the present situation to be one step before cybercriminals. Presently, the activities in this scope within the territory of a given country are not enough to effectively fight with the international cybercrime. However mental progress is visible among the international actors and it might shortly lead to the change of the present state of affairs in order to try to overtake cybercriminals. International cooperation may cause synergy effects to achieve the intended goals. The author called this kind of goals 2MKQ effect<sup>7</sup>. Such attitude would let us achieve more effective catching of cybercriminals and other actions in cyberspace. We would obtain up-to-date information about cyber threats and solutions which is necessary in the fast changing world. And finally, we would be quickly warned about the threats which would make law enforcement quicker. In the author's opinion the following sentence is very important nowadays: "International cooperation in the fight against cyber threats actually is very crucial. The sooner countries get along, the faster they will be competing against cybercriminals." This is very important for all countries for which cybersecurity is a vital issue.

---

<sup>7</sup> 2MKQ - **M**ore effective catching cybercriminals, **M**ore effective actions in cyberspace, **K**eeper current threat information up to date, **K**eeper current solutions up to date, **Q**uick warning of cyber threats, **Q**uick law enforcement.

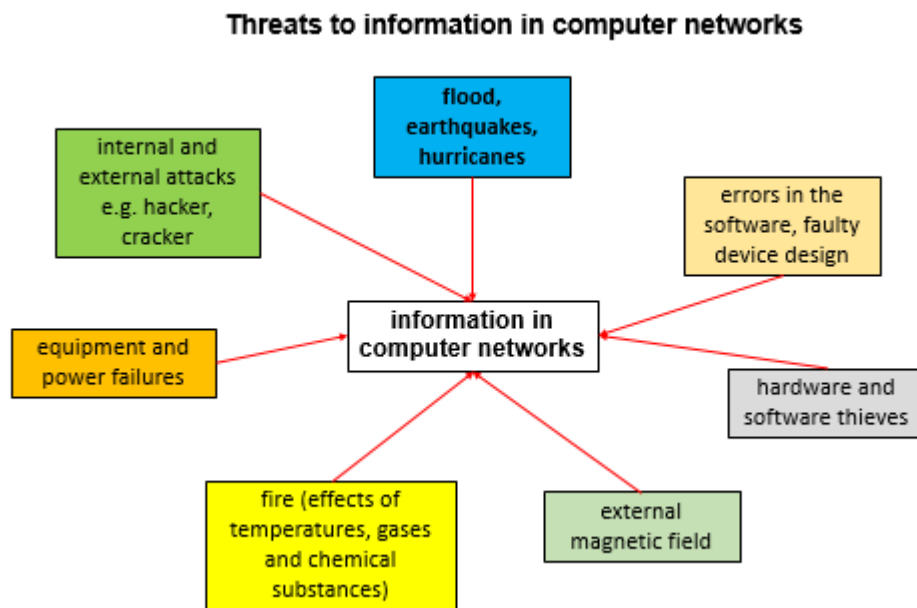


## ORGANIZATIONAL AND TECHNICAL CYBERSECURITY

First of all, people responsible for cybersecurity in a given organization should carry out an analysis of cyber threats which might occur. Figure 3 presents an example of threats to information in a computer network.

Fig. 3.

Example of cyber threats in a computer network



Source: Own elaboration.

Another aspect is paying attention to the approved security standards, where a vital rule says that: ICT systems which do not meet the relevant quality and reliability criteria should be returned for scrap.

ICT Security refers to all issues related to the security of IT systems and networks, in which information is generated, processed, stored or transmitted. It was assumed that an IT system is considered safe when it has the following attributes:

- confidentiality - sharing data only to authorized persons;
- integrity - protecting the system against unauthorized changes;
- availability of information - delivery in the required place and time;
- secretiveness - protection against unmasking;
- certainty of identification - reliable identification of system users;
- accountability - the possibility of determining all events that occurred in the system;
- controllability - the ability to check whether the security procedures established in the system are observed.

Taking into consideration the standards, it is necessary to pay attention to the rules of data processing in IT infrastructure. They are described in a document ISO/IEC 27000:2018 (Information technology — Security techniques — Information security management systems — Overview and vocabulary)<sup>8</sup>. Point 3.28 describes information security as preservation of confidentiality (3.10), integrity (3.36) and availability (3.7) of information.

Note 1 to entry: In addition, other properties, such as authenticity (3.6), accountability, non-repudiation (3.48), and reliability (3.55) can also be involved. The factors can be understood as:

- 3.10 confidentiality - property that information is not made available or disclosed to unauthorized individuals, entities, or processes;
- 3.36 integrity - property of accuracy and completeness;
- 3.7 availability - property of being accessible and usable on demand by an authorized entity;
- 3.6 authenticity - property that an entity is what it claims to be;
- 3.48 non-repudiation - ability to prove the occurrence of a claimed event or action and its originating entities;
- 3.55 reliability - property of consistent intended behaviour and results;
- 3.5 authentication - provision of assurance that a claimed characteristic of an entity is correct.

Another document includes the rules of data processing in IT infrastructure EN ISO/IEC 27002:2022 (Information security, cybersecurity and privacy protection — Information security controls)<sup>9</sup>. The document is a standard which is helpful in the implementation of an Information Security Management System (ISMS) based on ISO/IEC 27001. It is a benchmark, commonly acceptable guidelines concerning the management of information security including cyber risk. The document describes among others the following topics:

- Information security policies - Management direction for information security (point 5);
- Human resource security - Prior to employment, During employment, Termination and change of employment (point 7);

---

<sup>8</sup> See ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. Retrieved October 10, 2022 from: <https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27000:ed-5:v1:en>.

<sup>9</sup> See EN ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. Retrieved October 10, 2022 from: <https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27002:ed-3:v2:en>.

- Asset management - Responsibility for assets, Information classification and Media handling (point 8);
- Access control - Business requirements of access control, User access management, User responsibilities and System and application access control (point 9);
- Cryptography - Cryptographic controls (point 10);
- Physical and environmental security - Secure areas and Equipment (point 11);
- Operations security - Operational procedures and responsibilities, Production from malware, Backup, Logging and monitoring, Control of operational software, Technical vulnerability management and Information systems audit coordination (point 12);
- Communication security - Network security management and Information transfer (point 13);
- System acquisition, development and maintenance - Security requirements of information systems, Security in development and support processes and Test data (point 14);
- Information security incident management - Management of information security incidents and improvements (point 16).

Cybersecurity is based on:

- organizational security - including the connection of the technique used with the local conditions of the system environment (personal security, access control, security management);
- technical security – covering undertakings related to the application of technical means (software based security, cryptographic security, electromagnetic security, physical security).

Organizational security includes:

- personal security – applies to the introduction of personal security requirements that explicitly specify what qualifications, permissions should be included in the security personnel, technical staff or system user authorization;
- access control organizations – it concerns the application of the adopted procedures for controlling access to information and areas subject to special protection;

- safety management – applies to the use of automated safety management systems that perform specific functions according to the needs resulting from the safety analysis;
- security checks and training– includes conducting current, ad hoc, periodic and comprehensive security checks, as well as conducting employee training in the area of threats, procedures and principles of information protection, as well as familiarizing with legal aspects and criminal liability for violation of provisions on protection of information.

Technical security includes:

- software based security – relates to software data protection using access control, encryption control, information flow control and requesting;
- cryptographic security – it concerns protection against browsing and wiretapping making incomprehensible information by providing, among others: encryption of information, masking of traffic in the network and protection of information collected in databases of ICT systems;
- electromagnetic security – concerns the assurance of electromagnetic compatibility of the operation of systems and the limitation of electromagnetic leakage;
- physical security – includes the restriction of unauthorized persons to move around facilities in which computer systems are developed and installed, as well as traffic control of authorized persons.

The author in the article focused on technical issues concerning the provision of cybersecurity which will be presented in more detail in the further part of the article.

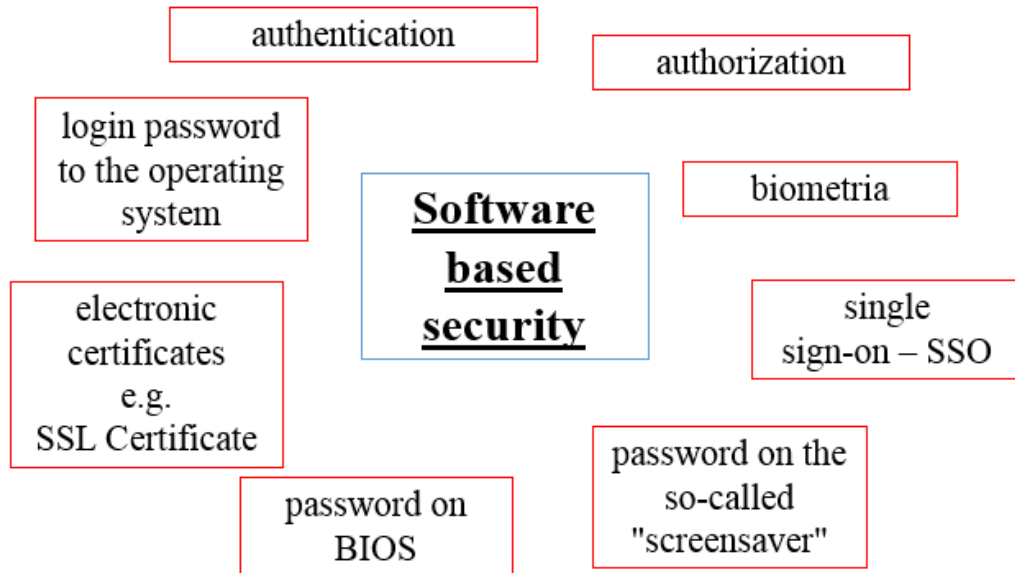
Software based security (see Fig. 4) includes the use of methods and program means that ensure the security of information generated, stored, processed and transmitted within the system. It includes four types of controls:

- access control – mechanisms for controlling access to objects, data of an automated command system;
- encryption control – security programs contain their own data files that control the process of encrypting and assigning specific keys;
- control of information flow – mechanisms determining the rules of access to facilities;

- controlling "requesting" – in the process of declassifying information, it should be ensured that classified information is not disclosed.

Fig. 4.

Technical tasks of software based security



Source: Own elaboration.

Software based security uses the authentication and authorization process:

- authentication is the process by which the declared identity of a person, device or service is verified;
- authorization is a process in which the confirmation of whether a given entity is entitled to use the requested resource.

It is very important to verify people who want to be inside the system (authorization and authentication) by:

- "something you have" - keys, magnetic cards;
- "something you know" - PIN, passwords, confidential data;
- "something you are" – biometric methods.

The most important safety rules in cybersecurity concerning human activities say:

- use strong passwords (preferably 14 characters) with symbols, no dictionary entries;
- do not use the option to remember your password;
- do not click on links from emails from an unknown source;
- use two-level verification when logging in;
- try not to use hot spots;

- use anti-virus programs.

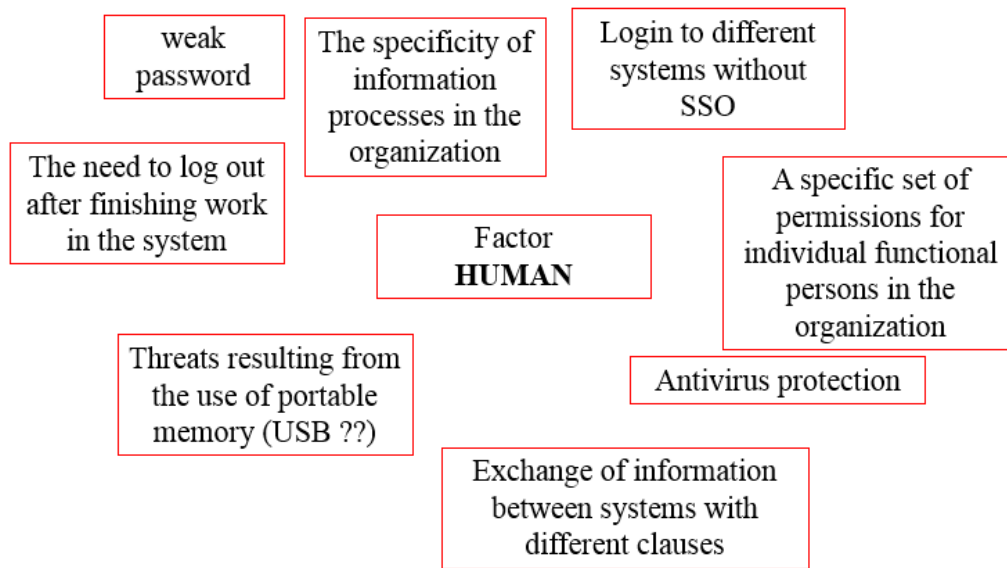
Many users find it difficult to create a password that would be easy for them and at the same time difficult to break, but it is enough to apply a few basic rules: a long password, for example, 14 characters; do not use dictionary words such as cat; a good password should contain letters, numbers and special characters; replace the letter with a digit such as A to 4 or E to 3; do not save passwords on a piece of paper (you can use password managers but encrypted); you can test the password in the password tester and remember that password consisting of your nick is bad, for example: NICK123 \*\*.

Nowadays, cyber specialists warn that the ID card can be: lost, destroyed, or it can be stolen thus the most convenient for the user are biometric methods, but they require the use of complicated and expensive equipment. The most well-known biometric methods include fingerprint scanning and evaluation of its details, so-called minutia. High hopes are also currently associated with the identification capabilities by analyzing the image of the iris or DNA.

The basic elements of cybersecurity relating to a human factor are presented on Figure 5. In cybersecurity a lot of emphasis is put on activities aimed at building the awareness of members of an organization, since taking into consideration the weakness of a human factor it is advised to stick to the statement that cybersecurity in an organization is as strong as the weakest element i.e. a human being. Thus, it is necessary to create proper conditions for organization's members so that their awareness in the scope of security is constantly on a high level and avoid situation when the weakness of a human factor can appear e.g. when personnel writes down their passwords on yellow papers due to the necessity to change their passwords too often.

Fig. 5.

Elements of cybersecurity related to the human factor



Source: Own elaboration.

Particular attention in terms of software based security should be paid to the determination of IP addressing in the area of local and wide area networks - the preferred solution for fixed addressing, VPN<sup>10</sup>, VLAN<sup>11</sup>, MAC addresses<sup>12</sup> and of course very important naming which is confidential information.

The next factor of technical security is cryptographic protection which consists of:

- encryption;
- using cryptographic mechanisms to integrate data;
- authenticated entities;
- authenticated information.

Cryptographic protection of an ICT system or network is used when transmitting information in electronic form outside security zones.

The following element of technical security is electromagnetic protection consisting of the placement of devices, connections and lines in security zones which guarantees compliance with the requirements of electromagnetic protection and the use of devices, connections and

<sup>10</sup> VPN - a virtual private network, allows you to use private network resources in the area of the public network.

<sup>11</sup> VLAN - a virtual Local Area Network (LAN), a computer network separated logically within a different, larger physical network.

<sup>12</sup> MAC address - media access control address is the unique address assigned to the network interface controller (NIC) in the production process.

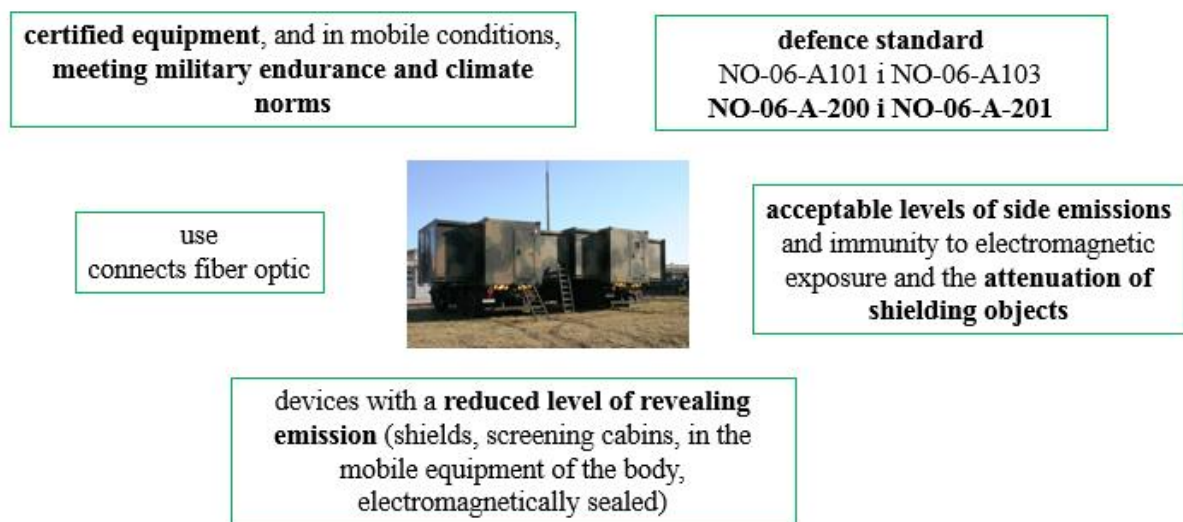
lines with a reduced emission level or their screening and filtering of external power and signal lines

Ways of preventing information leakage from side electromagnetic radiation include those which are presented on Figure 6.:

- screening rooms in which important information is processed;
- use of active devices with minimized electromagnetic emission level, e.g. TEMPEST technology device;
- active radio engineering masking;
- skillful arrangement of radiating elements in the administrative zone of an institution or enterprise.

Fig. 6.

Elements of cybersecurity related to electromagnetic protection



Source: Own elaboration.

Last but not least factor of technical security is physical security. The physical protection of an ICT system or network consists of:

1. Placing system devices or ICT network in the security, administrative zone or special security zone called "Controlled access zone" depending on:
  - classification of information, e.g. in secret systems;
  - the amount of information processed;
  - threats to the confidentiality, integrity or availability of information.
2. The application of measures ensuring physical protection in particular against:
  - unauthorized access;



- preview;
- wiretapping.

When developing the principles of physical security, the following criteria must be adopted for physical security:

- construction criteria;
- entrance door (Confidential);
- entrance door (Secret or Top secret);
- window openings, ventilation, etc.;
- windows;
- safes;
- rooms.

All elements must meet the requirements according to legal acts. The above criteria concern first of all a stationary infrastructure. While in mobile conditions, particular attention should be paid to other vital factors:

- VC (command vehicle), VCS (command and staff vehicle) and teleinformation equipment security;
- cabling control and introduction of links from the point of view safety and security requirements;
- security system by guards;
- restricted access zones;
- marking protection zones around command and control vehicles, in which classified information is processed;
- protection of the installation against natural disasters;
- ensuring the reliability of electricity and air conditioning sources;
- application of protection measures against unauthorized access to equipment and programs.

While realizing physical security it must be remembered that “your server is as secure as its physical protection”. This motto is very important for the assurance of cybersecurity due to the fact that if we have a physical access to an active infrastructure we can cause information leakage or taking control over the functioning of the computer network.

## CONCLUSION

The range of problem matter aiming at assuring cybersecurity, which is presented in the article, indicates that such an activity is not easy and it requires many factors to be met as well as all people functioning in a given organization to be involved. A human factor plays a vital role in the process of assuring cybersecurity, thus it is extremely important to keep social awareness on as high level as it is possible. Meeting the complex goals in organizational and technical terms requires the employment of certain staff specializing not only in the field of ICT but also in management, social behaviour as well as cyber risk. According to the author, the thesis statement presented at the beginning of the article is true, however it requires awareness that the described content should be treated only as some directions which should be taken into consideration in the process of providing cybersecurity. Finally, the author suggests to get acquainted with an interesting approach to cybersecurity presented below.

10 Immutable Security Rights<sup>13</sup>:

Right-1: if the attacker is able to convince you to install his program on your computer, it is not your computer anymore;

Right-2: if the attacker can change the operating system on your computer, it is not your computer anymore;

Right-3: if the attacker has unlimited physical access to your computer, it is not your computer anymore;

Right-4: if you let the attacker modify your website, it is not your website anymore;

Right-5: weak password destroys solid protection;

Right-6: computer security is directly proportional to the administrator's honesty;

Right-7: the security of encrypted data depends on the quality of the decryption key;

Right-8: the use of an outdated virus scanner is only slightly better than a complete lack of it;

Right-9: absolute anonymity is impractical in the real world and on the web;

Right-10: technology is not a panacea.

The above sentences confirm that a human being plays a vital role in cybersecurity and technology is not a panacea. Last but not least, according to the author the major rule when we want to ensure cybersecurity in a military hierarchical organization (and other) is common

---

<sup>13</sup> See 10 Immutable Security Rights. Retrieved October 20, 2022 from <https://www.linkedin.com/pulse/microsoft-technet-ten-immutable-laws-security-juergen-moy>.

sense and providing cybersecurity taking into consideration financial possibilities as well as the risk connected with data loss.

## REFERENCES LIST

### LITERATURE

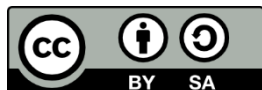
- Kissel R., Glossary of Key Information Security Terms, National Institute of Standards and Technology, May 2013.  
Pilarski G., Ochrona informacji w sieciach komputerowych, AON, Warszawa 2004.  
Pilarski G., Tackling cyberspace threats – the international approach, Security and Defence Quarterly, 2016, Volume 3, No. 12.

### SOURCES

- Decyzja Nr 275/MON z dnia 13 lipca 2015 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej.  
EN ISO/IEC 27002:2022 Information technology — Security techniques — Code of practice for information security controls.  
ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary.  
Ustawa z dnia 5 lipca 2018 r. - o krajowym systemie cyberbezpieczeństwa (Dz. U. Nr 2018, poz. 1560).  
Ustawa z dnia 30 sierpnia 2011 r. - o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. 2011 nr 222 poz. 1323).  
Ustawa z dnia 17 lutego 2005 r. - o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2021 poz. 2070, z 2022 r. poz. 1087).  
Ustawa z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.)  
Ustawa z dnia 15 września 2017 r. - o stanie klęski żywiołowej (Dz.U. 2017 poz. 1897).  
Ustawa z dnia 21 czerwiec 2002 r. - o stanie wyjątkowym (Dz.U. 2017 poz. 1928).



Copyright (c) 20022 Grzegorz PILARSKI



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.