DOI 10.5817/MUJLT2023-2-5

CYBERSECURITY: NOTORIOUS, BUT OFTEN MISUSED AND CONFUSED TERMS*

by

JAN KOLOUCH † DANIEL TOVÁRŇÁK ‡ TOMÁŠ PLESNÍK § MICHAL JAVORNÍK ¶

The article deals with the issue of the terminology used in the implementation and provision of cyber and information security. Although this terminology is understood as notoriety, practice shows that there are different perspectives on defining "the same". Nowadays, mainly in the context of the adoption of Directive (EU) 2022/2555 of the European Parliament and of the Council on measures to ensure a high common level of cybersecurity in the Union (NIS 2), there is a need for a consistent interpretation and, in particular, understanding of the terminology used so that cybersecurity and information security can be truly ensured. After analyzing and comparing the various definitions, the paper presents clear, general but universally applicable definitions of key terms. The relationship of these terms is presented within a conceptual model and also through a practical example.

KEY WORDS

Cybersecurity, Information security, Event, Threat, Asset, Vulnerability, Risk, Control, Information Security Management System, security terminology

* This article was supported by the European Regional Development Fund "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

† jan.kolouch@law.muni.cz, CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence (C4e), MUNI; jan.kolouch@cesnet.cz, CESNET a.l.e., Czech Republic

‡ tovarnak@ics.muni.cz, CSIRT-MU, MUNI, Czech Republic

§ plesnik@ics.muni.cz, CSIRT-MU, MUNI, Czech Republic

¶ javornik@ics.muni.cz, CSIRT-MU, MUNI, Czech Republic

1. INTRODUCTION

In a relatively short period, contemporary society has been exposed to very intense changes related to the massive integration of information and communication technologies[1] into most areas of human activity. Dependence on ICT has reached an imaginary „event horizon" and humanity can no longer able to exist without these technologies. This dependence naturally brings with it a huge scope for cyber threats, attacks, and crime. We can observe a trend of traditional security threats[2] moving into cyberspace, creating new threats specific to this environment. There is also a stronger intermingling of different threats and a hybridization of the security environment, the dynamics and scope of which are enhanced by cyberspace and ICT.

It is necessary to respond to these negative phenomena and create space for the implementation of cybersecurity and information security principles at all levels, in all affected processes, and towards all stakeholders.

When we talk about cyber security, it is important to remember that we are in an area where the terms „information and communication technology security", „cyber security" and „information security" are often confused as synonyms. In practice, it is often possible to try to specify these terms and their boundaries precisely[3], but this is not the aim of the present article, since the terminology discussed in this article can be applied in all these areas.

In very simplistic terms, ICT security is the set of measures, procedures, and practices applied by individuals or organizations to ensure the triad of CIA (confidentiality, integrity, and availability) of these systems and the data they contain. ICT security monitors the security of both the entire ICT infrastructure and individual endpoint devices.

Cybersecurity is a relatively comprehensive system including technical, organizational, and other measures to protect ICT, applications, data, and users. Cybersecurity should also be seen as the ability to respond to cyber threats or attacks and their consequences, as well as planning for the recovery

---

1 Hereinafter referred to as ICT

2 For example: *Cyber-attacks have tripled in past year, says Ukraine's cybersecurity agency* [online]. The Guardian. Available from: `https://www.theguardian.com/world/2023/jan/19/cyber-attacks-have-tripled-in-past-year-says-ukraine-cybersecurity-agency` [Accessed 20 February 2023], *Russia's war on Ukraine: Timeline of cyber-attacks* [online]. European Parliament. Available from: `https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549` [Accessed 20 February 2023], *Industroyer2: Industroyer reloaded* [online]. Eset. Available from: `https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/` [Accessed 20 February 2023]

3 See e.g.: Solms, R.V., & Niekerk, J.F. (2013). *From information security to cyber security. Comput. Secur., 38, 97-102.*

of the functionality of these systems and the services associated with them, including the final learning from a crisis.[4]

Information security is primarily focused on the protection of information, regardless of the type of medium (paper, electronic media, etc.) or the system in which the information is processed. Information security is then applied to information throughout its life cycle.

Even though the term „information security " is more commonly used as a „superordinate " term in the professional literature and technical standards (see Chapter 2), the term „cybersecurity " will be used as a general term in this article, especially because of the EU legislative framework, where this term is the superordinate or umbrella term.[5] Where necessary to present different approaches, both the terms cybersecurity and information security will be used.

An integral part of information and cybersecurity is the terminology that is used in ensuring this security. This terminology is all the more important as it is part of the legislation adopted at both national and international levels. Earlier this year, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity in the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [6] entered into force. This directive uses terminology that is often based on technical standards, but when translated into legal language, the use of this technical terminology is often not entirely appropriate, often even incorrect. In practice, there is a clash between the views of engineers, security personnel, and lawyers, who define a relatively clear concept quite differently.

It is not possible to define all the terms related to cyber security (e.g. cyber attack, cyber threat, significant cyber threat, threat actor, near miss, eventuality, etc.) and to cover in detail all the technical and legal implications

[4] Kolouch, J. and Bašta, P. (2019) *CyberSecurity*. Praha: CZ.NIC. ISBN 978-80-88168-31-7. p. 44-45.

[5] See e.g.: European Commission. (2022)*The Cybersecurity Strategy* [online]. European Commision. Available from: `https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy` [Accessed 8 August 2023], Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity in the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[6] Hereinafter referred to as NIS 2. Available from: `https://eur-lex.europa.eu/eli/dir/2022/2555/oj`

of the terminology used. For this reason, the authors have focused on the "key" terms and their interrelationships (see Chapter 3). The presented outputs can then be further supplemented with additional terminology and interrelationships can also be added to the presented Conceptual Model. Based on the comparison, the authors try to point out the shortcomings and differences in the technological and legal understanding of the terminology used, while their own opinions and de lege ferenda suggestions on individual legal and technical definitions are also presented.

The purpose of the presented article is not to find a single suitable or universal explanation of the given terms, as such a solution de facto does not exist. It is also not to create new terminology or definitions of existing terms, but rather to find a consensus or at least to define a generally accepted framework of the given terminology for technical, legal, and user purposes.

2. EVOLUTION OF THE LEGAL FRAMEWORK FOR CYBERSECURITY REGULATION

One of the first definitional standards that addressed the issue of security as well as defining terminology in the online environment was the RFC (*Request For Comments*)[7]. Although these documents are recommendations rather than standards, they are respected by users as if they were standards.[8]

These standards created a general premise for the creation of other, more detailed technical and legal standards defining the basic terminology of cyber and information security.

Information security is also defined by ISO 27000 standards. Information security standards related to this article include:

- ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary[9]

[7] RFC documents contain technical specifications and organizational notes for the Internet. The RFCs are freely available at: `https://www.ietf.org/rfc/`

[8] Security related RFCs include mainly: RFC 1208 (A Glosary of Networking Terms), RFC 1983 (Internet Users' Glossary), RFC 4949 (Internet Security Glossary), RFC 2196 (Site Security Handbook), RFC 2350 (Expectations for Computer Security Incident Response), RFC 2504 (Users' Security Handbook), RFC 3631 (Security Mechanisms for the Internet), RFC 6040 (Security Architecture for the Internet Protocol), RFC 4778 (Current Operational Security Practices in Internet Service Provider Environments). The RFCs are freely available at: `https://www.ietf.org/rfc/`

[9] Hereinafter referred to as ISO/IEC 27000. Available from: `https://www.iso.org/standard/73906.html`

- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements[10]
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls[11]
- ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks[12]

At the level of the European Union, it has long been possible to observe efforts to protect the assets of cyberspace and, at the same time, to harmonize the legislation of individual Member States so that the issue of cybersecurity can be effectively addressed. The first steps in this area can be traced back to the 1990s[13] and then to the beginning of this millennium.[14] The most significant change was brought about by Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union[15], which is currently still in force.

The European Parliament adopted on 10 November 2022 and the Council of the European Union on 28 November 2022 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). As this is a Directive, not a Regulation, the legislative process for adopting the Directive is not yet complete. The

[10] Hereinafter referred to as ISO/IEC 27001. Available from: https://www.iso.org/standard/82875.html

[11] Hereinafter referred to as ISO/IEC 27002. Available from: https://www.iso.org/standard/75652.html

[12] Hereinafter referred to as ISO/IEC 27005. Available from: https://www.iso.org/standard/80585.html

[13] E.g. Directive 91/250/EEC of the European Parliament and of the Council on the legal protection of computer programs. Council Decision 92/242/EEC on the security of information systems.

[14] E.g. Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce), Directive 2002/19/EC of the European Parliament and of the Council on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), Regulation 460/2004/EC of the European Parliament and of the Council establishing the European Network and Information Security Agency, as amended by Regulation 1007/2008, Directive 2008/114/EC of the European Parliament and of the Council on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[15] Hereinafter referred to as NIS 1. Available from: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:32016L1148

Directive entered into force on 16 January 2023 and individual Member States have 21 months from that date to implement the Directive in their legal systems (expected October 2024). The NIS2 Directive aims to strengthen EU cybersecurity and harmonize the rules for ensuring it across the EU. The Directive, therefore, brings modifications to existing requirements and extends regulation to several new organizations and other changes.

In addition to these standards, the terms (typically in the form of explanatory dictionaries) related to the issue of information and cybersecurity are also defined by organizations that, based on their mandate, have a certain privileged position in this area. These organizations include in particular The European Union Agency for Cybersecurity (ENISA)[16], the Cybersecurity & Infrastructure Security Agency (CISA),[17] and the National Institute of Standards and Technology (NIST)[18].

All the technical and legal documents mentioned above very often work with terms that will be defined in the following chapter. However, these terms are not used doctrinally and uniformly. On the contrary, they are often used synonymously and are also often overused in situations where their use is inappropriate. This degree of linguistic creativity can be observed both at the international and, in particular, at the national level in the context of the transposition of EU legal norms into national legislation.

For this article, definitions based on ISO/IEC 27000, NIST, CISA, NIS 1, and NIS 2 will be used in the remainder of this article. The authors are aware of the existence of other standards or technical interpretative dictionaries, but the aim is to highlight the ambiguity in the interpretation of key cyber and information security concepts, both within and outside the European Union. A secondary objective is to highlight the not-always-clear and unambiguous terminology presented within the NIS2.

3. THREAT, ASSET, VULNERABILITY, RISK, EVENT, AND MORE

In this part of the article, attention will first be paid to the characteristics of six key terms (Asset, Event, Threat, Vulnerability, Risk, and Control) related to cybersecurity. The terminology used in both legal and technical

[16] *Glossary* [online]. ENISA. Available from: `https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary` [Accessed 10 January 2023].

[17] *Explore Terms: A Glossary of Common Cybersecurity Words and Phrases* [online]. NICCS. Available from: `https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary` [Accessed 10 January 2023].

[18] *Guide for Conducting Risk Assessments: Information Security* [online]. NIST. Available from: `https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf` [Accessed 10 January 2023].

standards is often imprecise, incomplete, and sometimes contradictory. These shortcomings result in a misunderstanding of security management as a whole.

Based on the comparison made, the authors try to point out the shortcomings and differences in the technological and legal concept of the terminology used, while their own opinions and suggestions de lege ferenda on individual legal and technical definitions are also presented.

The relationship and interrelationship of these key and other concepts will then be presented within the framework of a conceptual model. This model provides a basic framework into which further sub-relationships can be added.

3.1. ASSET

An asset can be a tangible thing (a building, computer system, network, energy, goods, etc.) or intangible (information, knowledge, data, programs, etc.) from the perspective of civil law. However, an asset can also be a property (e.g. availability and functionality of a system and data, etc.) or a good name, reputation, etc. People (users, administrators, etc.) and their knowledge and experience are also an asset from a cybersecurity perspective. ISO/IEC 27000 does not define the term „asset" itself, but states that „information is an asset that, like other important business assets, is essential to an organization's business and, consequently, needs to be suitably protected." [19] It follows, therefore, that the term „asset" is primarily related to the concept of information or other assets important from a business perspective. However, it is questionable whether all assets of an organization must necessarily fulfill the condition of a relationship to information or business.

Another definition of „asset " can be found in ISO/IEC 19770-1 (IT asset management), which states that an „asset " is an item, thing, or entity that has potential or actual value to an organization.

According to NIST the „asset" is a „major application, general support system, high impact program, physical plant, mission-critical system, personnel, equipment, or a logically related group of systems."[20] It is clear that the NIST definition of „assets" is quite inadequate, as it focuses only on systems (hardware and software) and personnel. No consideration is given to the value of data, information, etc.

[19] ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. p. 12.

[20] CNSS. *Committee on National Security Systems (CNSS) Glossary* [online]. Available from: `https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf` [Accessed 10 January 2023].

NIS 1 and NIS 2 directives do not define the term „asset", although the term asset is used in both legal standards. NIS 2 Article 7, point (9), letter (d) sets out the obligation to establish „a mechanism to identify relevant assets and an assessment of the risks in that Member State". Similarly, Article 9, point (3) provides that Member States are to identify „assets that can be deployed in the case of a crisis for the purposes of this Directive."

CISA states that the asset is „a person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value." Extensively, an asset can be considered as „anything useful that contributes to the success of something, such as an organizational mission; assets are things of value or properties to which value can be assigned."[21]

Similarly, an asset is defined in ISO/IEC PDTR 13335-1, which states that an asset is „anything that has value to the organization, its business operations, and their continuity, including Information resources that support the organization's mission."

Both definitions are sufficiently general to include assets that are significant to the person who manages or owns them. When it comes to defining or identifying an asset, the determining factor is first and foremost the objectives of the organization, which determine what the primary assets are (processes/activities and information) and then also what the main risks to those assets are from the sources of uncertainty (threats and opportunities).

As NIS 2 does not define the actual concept of an asset, different countries may have different implementations of what will be considered an asset. Thus, for example, information and services may be considered assets in one national legislation and only data and processes in another. This disparity may have a significant impact on the identification of assets, especially if the subject implementing the cybersecurity rules uses, for example, the services of multinational corporations or organizations based abroad, i.e. under different legislation. A separate issue is how the different legal regulations deal with the identification of primary and supporting assets (e.g. ICT technologies, employees, objects, etc.).

Based on a comparison of these definitions and the absence of a general legal definition, we believe that it would be appropriate to provide that an asset is anything that has value and contributes to the achievement of an organization's objectives.

[21] NICCS. *Explore Terms: A Glossary of Common Cybersecurity Words and Phrases* [online]. NICCS. Available from: `https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary` [Accessed 10 January 2023].

In the case of an asset, the authors prefer the definition given in ISO/IEC 19770-1, but in addition, the asset needs to be consistently mapped to the organization's objectives. This is because, according to the authors, it is not possible for an organization's objective to exist without the support of at least one asset and, conversely, an asset is not an asset if it does not support at least one of the organization's objectives.

For example, if the organization in question is in the business of providing data storage services through a privately-owned data center, the typical asset inventory would include the actual data center facility, i.e., the building, and the storage servers.

3.2. EVENT

An event could be defined as a situation that has occurred or is believed to have occurred.

According to ISO/IEC 27000, an event is an „occurrence or change of a particular set of circumstances". Bearing in mind that an event can consist of something not happening. ISO/IEC 27000 states that „an event can sometimes be referred to as an „incident" or „accident".

NIST defines an event as „any observable occurrence in a network or system."[22] CISA defines „event" very similarly, stating that it is an „observable occurrence in an information system or network." Relating an event to the concept of „any observable occurrence" is, in our opinion, misleading for several reasons. There may be a situation where an event is not observable (for whatever reason), and under this interpretation, it would then obviously not be an event. Also, the event is only related to the „network, system, information system" environment thus creating a relatively small ecosystem for the possibility of an event to occur.

NIS 1 Directive does not define the term event in any way, but only states that:

- „Risk means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems"[23];
- „Incident means any event having an actual adverse effect on the security of network and information systems"[24];

[22] Cichonski, P. et al. (2012) Computer Security Incident Handling Guide [online]. *NIST Special Publication (SP)*, 800-61 Rev. 2. Gaithersburg, MA: National Institute of Standards and Technology. Available from: doi: https://doi.org/10.6028/NIST.SP.800-61r2 [Accessed 10 January 2023]. p. 60.

[23] Article 4, point (9) NIS 1.

[24] Article 4, point (7) NIS 1.

based on the above, it can be concluded that both incident and risk (see below) are always an event according to NIS 1.

The definition of „event" is similarly handled in NIS 2, which states in Article 6, point (6) that „**incident means an event** compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems."

Thus, the term „event" becomes synonymous with the term „incident" according to the legislator. The authors do not believe that it is appropriate to draw an equivalence between the term „event" and „incident". The event can lead to action and, at the same time, can cause harm. The event could also pose a potential threat.

An example of an event is a planned entry of the service personnel onto the premises of the organization's data center. However, since the entry was planned and authorized according to the organization's policy, this event cannot be considered an incident.

Based on the above comparison, we believe that the term „event" should be rather defined as a situation that has occurred or is believed to have occurred. This presumption is there because there is a direct or indirect indication that the event has occurred.

In addition to the event, it is also possible to work with the concept of a non-event, i.e., the state or assumption that the situation did not occur. An event can be certain or uncertain.

Based on a comparison of these definitions and the absence of inconsistencies in the legal definition, we believe it would be appropriate to provide that an event is an occurrence or change of a particular set of circumstances within a particular domain; it is something that has happened, or it is contemplated as having happened in that domain.

The authors have extended the definition of the event[25] with two additional ideas as described by Etzion[26]. First, the notion of a domain is added, e.g., cybersecurity. This means that events that are not relevant to a particular domain might not be considered at all, rendering all events relevant. Second, an event is something that has happened or is contemplated as having happened. Thanks to this, it is possible to work with occurrences that are believed to have happened based on some indicators, even though further investigation may indicate the opposite, i.e., a false positive. Please note that an event is something that has already happened, i.e., it is in the

[25] ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection - Guidance on managing information security risks.

[26] Niblett, P., Etzion, O. (2010) *Event Processing in Action*. Manning. ISBN 9781638352624.

past. To refer to a hypothetical or potential event, i.e., one that is in the future, we will use the term **eventuality**. The eventuality is the source of uncertainty, which, as we will explain later, is an important concept underlying a risk. In addition, the event can have one or more **consequences**, i.e., outcomes that are directly or indirectly affecting objectives. Last, but not least, the event can usually denote an atomic occurrence, sometimes referred to as a simple event, or a composition of several events of arbitrary complexity, sometimes referred to as a situation or complex event.

3.3. THREAT

A threat can probably be most simply defined as an eventuality capable of disrupting the normal or orderly state of affairs. It is a negative action that may or may not be completed. For the actual definition, it is sufficient that the possibility of a negative state of affairs is imminent and real.

A somewhat different definition can be found in ISO/IEC 27000, where the threat is defined as a „**potential cause of** an unwanted **incident**, **which can result in harm** to a system or organization." A threat is therefore related to an incident that can lead to harm, which is related only to defined areas: a system or an organization (person or group of people).

According to NIST the threat „is any **circumstance or event** with the **potential to** adversely **impact** organizational operations and assets, individuals, other organizations, or the Nation through an Information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service."[27]

In defining the term threat, another related term is used: „event". The use of this term can be confusing as "threat manifests as an event which causes harm to asset". There is also a flaw in this definition in that the authors have not attempted to provide a general characterization of assets, but have instead defined various protected objects, whereas the phrase „potential to adversely impact assets" would have sufficed. We also have a negative view of the attempt to define the various types of „attack" or „harm type". The above list is exhaustive, but it is clearly not exhaustive.

NIS 1 and NIS 2 directives do not define the term „threat", although the term cyber threats are used in both legal norms. The legislator somewhat works with the term „threat" as a notoriety. NIS 2 in Article 6, point (10) states that „cyber threat" means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881.

[27] Cichonski, P. et al. (2012) Computer Security Incident Handling Guide [online]. *NIST Special Publication (SP)*, 800-61 Rev. 2. Gaithersburg, MA: National Institute of Standards and Technology 2012. Available from: doi: https://doi.org/10.6028/NIST.SP.800-61r2 [Accessed 10 January 2023]. p. 8.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) defines „cyber threat" as any **potential circumstance, event** or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.

In defining the term threat, the term „event" is again used inappropriately. At the same time, the term „action" is used, from which it is possible to infer an active action of, for example, an attacker. If we were to define the relationship between threat and action, it would be correct to state that „threat manifests as event and can lead to action".

The use of the adjective „cyber" in defining the term led the authors to believe that „threat" refers only to the impact on „network, information systems and the users of those systems". However, the question is whether the use of the prefix „cyber" is appropriate or whether, on the contrary, it further complicates the established, albeit largely inaccurate, terminology. The word cyber refers primarily to the relationship to cybersecurity, but the area that is protected against threats is at least in the scope of information and cybersecurity, but in a broader sense it can also protect against physical threats that do not originate from the digital environment but are capable of negatively affecting this environment.

The impact on „other persons" can then be seen as an expansive interpretation of the impact of this cyber threat. On the negative side, the attempt to define the different types of „harm type" can again be seen, although the use of the phrase „or otherwise adversely impact" makes it a more appropriate classification than in the previous case.

According to CISA, a „threat" is a „circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society."[28]

As in the previous cases, the term „event" is inappropriately used, but „potential to exploit vulnerabilities and to adversely impact assets" is appropriately used. This definition is probably the closest to a general and non-deceptive definition of „threat".

[28] NICS. *Explore Terms: A Glossary of Common Cybersecurity Words and Phrases* [online]. NICCS. Available from: `https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary` [Accessed 10 January 2023].

A typical example of a threat is the eventuality of a fire. A threat may also be, for example, unauthorized access to data center premises.

Comparing all these definitions, it can be concluded that a threat is an eventuality that can be expected to have negative consequences for the objectives.

At the same time, the negative consequences, or **harm, always act on objectives** through the underlying assets. It should also be noted at this point that in practice the terms threat and threat agent/actor are often confused. The realization of a threat can only occur if there is a corresponding vulnerability that it exploits and a threat actor that can exploit it. Although a threat represents a source of uncertainty, its existence is de-facto immutable. This means that to reduce the likelihood of a threat materialization, or its consequences, appropriate measures are addressing the vulnerability, and the harm, respectively, but never directly the threat itself.

3.4. VULNERABILITY

Vulnerability refers to a weakness in an asset or security that is exploited by one or more threats. Vulnerability defined in this way more or less corresponds to the definition according to ISO/IEC 27000, but instead of the term security, the term „control" is used, which is characterized as „a measure that is modifying risk". According to a semantic interpretation, it would be possible to accept the interpretation that the term „measure that is modifying risk" is de facto a certain security measure.

Another definition of „vulnerability" can be found in ISO/IEC 27005, which defines „vulnerability" as a weakness of an asset or control that can be exploited so that an event with a negative consequence occurs.

NIST defines a vulnerability as „a weakness in a system, system security procedure, internal controls, or implementation that could be exploited by a threat source."[29] This definition is based on the assertion that „most information system vulnerabilities can be associated with security controls that either have not been applied (either intentionally or unintentionally), or have been applied, but retain some weakness. However, it is also important to allow for the possibility of emergent vulnerabilities that can arise naturally over time as organizational missions/business functions evolve, environments of operation change, new technologies proliferate, and new threats emerge. In the context of such change, existing security controls may become inadequate and may need to be reassessed for effectiveness. The

[29] Cichonski, P. et al. (2012) Computer Security Incident Handling Guide [online]. *NIST Special Publication (SP)*, 800-61 Rev. 2. Gaithersburg, MA: National Institute of Standards and Technology. Available from: doi: https://doi.org/10.6028/NIST.SP.800-61r2 [Accessed 10 January 2023]. p. 9.

tendency for security controls to potentially degrade in effectiveness over time reinforces the need to maintain risk assessments during the entire system development life cycle and also the importance of continuous monitoring programs to obtain ongoing situational awareness of the organizational security posture."[30]

Directive NIS 1 uses the term vulnerability only in Recital 59, which states that „CSIRTs should pay particular attention to the need to keep information about product vulnerabilities strictly confidential, prior to the release of appropriate security fixes." This interpretation, therefore, suggests that the legislator applies the concept of vulnerability only to „products" in the current and effective Directive. Such a characterization of vulnerability is inadequate and certainly does not help to create legal certainty.

In the NIS 2 directive, the actual concept of vulnerability is mentioned in Article 6, point (15), where it is stated that „vulnerability means weakness, susceptibility or defect in ICT products or ICT services that can be exploited by a cyber threat".

The question is why the legislator is introducing a new concept of „susceptibility", which is to a large extent even broader than the concept of „weakness". The term „susceptible" generally means that a person, thing, or situation tends to be more susceptible or more prone to a particular type of behavior or event. For example, a person may be prone to being overweight, meaning they are more likely to become obese if they do not take care of their diet and physical activity. Similarly, an area may be prone to earthquakes, which means that there is a greater likelihood of earthquakes occurring there compared to other areas. The term „weakness" usually means a deficiency or weakness in a particular area. For example, a person may have a weakness in mathematics, which means they have difficulty understanding and solving mathematical problems. Similarly, a person may have a weakness in a security system, which means that the system has deficiencies or vulnerabilities that could be exploited for attack or attack. Both terms refer to specific flaws or problems, but the term „susceptibility" focuses on the tendency for a particular behavior or event to occur, while „weakness" focuses on specific flaws or vulnerabilities in a system or area.

As regards the definition of the range of assets, i.e. „ICT products or ICT services", we believe that such a significant narrowing of the potential impact of the vulnerability is completely inappropriate. It would certainly be more appropriate to use the more general term „asset" instead of „ICT products

[30] *Op. cit.* p. B-13. Also see: *Committee on National Security Systems (CNSS) Glossary* [online]. Available from: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf [Accessed 10 January 2023] p. 131.

or ICT services". The narrowing down to only „cyber threat" should also be criticized (see the analysis of the definition of a threat).

CISA describes vulnerability as a „weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source."

Even this definition shows a not entirely logical narrowing of the possible impact of vulnerability to only „information system, system security procedures, internal controls, or implementation".

A typical case of weakness is improper access control, when, for example, a software product does not restrict or incorrectly restrict access to a resource from an unauthorized actor. It becomes a vulnerability when the malicious actor finds an actual way to compromise the security of the product by gaining privileges, reading sensitive information, or executing commands, i.e., the weakness becomes exploitable.

Based on a comparison of these definitions, we believe that vulnerability should be understood as a weakness of an asset or control that can be exploited by a threat.

In the case of vulnerabilities, authors follow ISO/IEC 27005 almost verbatim but emphasize the relationship between the eventuality (threat) and the event. By the standard, it is needed to consider that both assets, e.g., processes, software, or hardware, and applied controls themselves, e.g., policies and rules, can be vulnerable (weak) concerning some threat. One can also say that vulnerability weakens assets and/or controls just enough so that some threat can materialize.

3.5. RISK

Risk is usually assessed as a combination of the probability that an adverse event (a harmful impact on a person, thing, or process, i.e., an asset) will occur and its impact if it does occur.

The risk assessment is usually based on three basic questions:

- What bad (undesirable) things can happen? What can fail?
- What is the possibility/probability of this happening?
- How severe (intensity, magnitude, etc.) can the effects (impacts, consequences) be?

Risk is also defined by various authors as the equation: **risk = impact * threat * vulnerability**. While this simplification is commonly used, it can be highly misleading and in the context of this article is rather discouraging.

A meaningful, defensible, and realistically applicable risk quantification principle for risk management can be a very complicated matter. It must

be understood that vulnerability and threat generally refer to a different asset than the impact of the potential exploitation of that vulnerability. An institution with a trivial asset structure will hopefully be able to get by with a simple formula; a more complicated institution will require more complex considerations.

Uncertainty plays a crucial role in quantifying risk. Based on the structure of the assets, it is necessary to infer which assets representing the organization's objectives will be impacted by the potential exploitation of vulnerabilities in the assets representing the supporting assets and what the level of such impacts will be. The second component of uncertainty that enters into the risk calculation is determining the probability that the exploitation of the vulnerability will occur.

„Risk is the effect of uncertainty on objectives[31]. In the context of information security management systems, information security risks can be expressed as an effect of uncertainty on information security objectives. Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization." [32]

NIST defines risk as „a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

(i) the adverse impacts that would arise if the circumstance or event occurs; and

(ii) the likelihood of occurrence."[33]

In defining risk, both definitions work consistently with the concept of „uncertainty". Uncertainty is the deficiency of information, understanding, or knowledge related to a potential event (eventuality). This may include the specific nature of the event, its consequences, or likelihood.[34]

[31] Objectives are results which should be achieved. Objectives can be strategic, tactical, or operational and can to different disciplines (e.g safety, financial, health) and can apply at different levels (strategic, organization-wide, project, product and process).

[32] ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. p. 8.

[33] Cichonski, P. et al. (2012) Computer Security Incident Handling Guide [online]. *NIST Special Publication (SP)*, 800-61 Rev. 2. Gaithersburg, MA: National Institute of Standards and Technology. Available from: doi: `https://doi.org/10.6028/NIST.SP.800-61r2` [Accessed 10 January 2023]. p. B-9.

[34] See also: NIST. (2019) Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. [online]. *NIST Special Publication (SP)* 800-37 Rev. 1 Gaithersburg, MA: National Institute of Standards and Technology.

According to Article 4, point (9) of the NIS 1, risk means „any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems."

In cyberspace, both users and the computer systems and applications that use them, as well as other ICT elements, are at risk. In our opinion, a narrow definition of risk only concerning the security of networks and information systems is therefore insufficient.

NIS 2 defines the concept of risk in a significantly different and to some extent „innovative" but at the same time quite confusing way. Article 6, point (9) states that risk means „the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident".

The risk itself relates only to the possibility of loss or disruption, presumably of an asset, following an incident. The question is whether only assets can be affected by risk or also objectives, as specified in ISO/IEC 27000. Quite inappropriately, then, the legislator directly associates risk only with the incident.

CISA defines risk as a „potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences." Similar to NIS 2, there is a linking of risk with „incident, event, or occurrence", but the above is linked to a particular threat. Such a definition is certainly more appropriate and accurate, even though it is not entirely correct.

The concept of risk itself is probably the most difficult to define. In terms of generality, the most appropriate definition is derived from ISO/IEC 27000, i.e., which states that „risk is the effect of uncertainty on objectives".

Having analyzed the above, we believe that risk can be understood as the effect of uncertainty, resulting from the lack of information related to the specific nature, likelihood, and consequences of an eventuality on the objectives.

The above-mentioned definition is based on the ISO/IEC 27000 and ISO 31000 Risk Management standards, where we only refine our understanding of the source of uncertainty, i.e., the eventuality. It should be pointed out that the abovementioned understanding, like the intent of the original definition, allows to work with positive risk, i.e., also with eventualities that can be expected to have positive consequences for the organization's objectives. In contrast with threats, such eventualities are commonly referred to as opportunities.

For example, a successful standardization of a new cryptography standard might be an opportunity with positive consequences for an organization's information security objectives, e.g., the confidentiality and integrity of data at transit/at rest. However, at the same time, an eventual vulnerability (presently unknown) of the standard might be considered potentially exploitable, thus giving rise to risk.

3.6. CONTROL

The control modifies either the consequences of the event or the vulnerability (reducing the likelihood of exploiting the vulnerability or possibly the impact and scope).

ISO/IEC 27000 states that „control is a measure that is modifying risk."[35] The control includes any process, policy, device, practice, or other actions which modify risk. The control itself may not always have the intended or anticipated modifying effect.

NIST defines common control „as part of the information security architecture, organizations are encouraged to identify and implement security controls that can support multiple information systems efficiently and effectively as a common capability (i.e., common controls). When these controls are used to support a specific information system, they are referenced by that specific system as inherited controls. Common controls promote more cost-effective and consistent information security
across the organization and can also simplify risk management activities."[36]

The NIS 1 and NIS 2 directives do not define the term „ control" although they work with this term. For example, NIS 2 in Recital 79 states that „...and have in place appropriate access control policies. Those measures should be consistent with Directive (EU) 2022/2557". In both directives, either the term control is used synonymously instead of „security requirements" or „measures".

CISA also does not characterize the concept of control and, similarly to the above-mentioned legal norms, uses the terms: measure, protective measure, and countermeasure in various forms. It is possible to assume that this is an attempt to describe the term „control" in a different manner.

[35] ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. p. 3.

[36] Cichonski, P. et al. (2012) Computer Security Incident Handling Guide [online]. *NIST Special Publication (SP)* 800-61 Rev. 2. Gaithersburg, MA: National Institute of Standards and Technology. Available from: doi: `https://doi.org/10.6028/NIST.SP.800-61r2` [Accessed 10 January 2023]. p. 16. See also: NIST. (2019) Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. [online]. *NIST Special Publication* (SP) 800-37 Rev. 1 Gaithersburg, MA: National Institute of Standards and Technology. p. B-9.

A typical example of a measure is the introduction of access control to the data center by authorizing authorized persons, granting access cards, controlling access to the data center using a camera system, etc.

By comparing these definitions, it can be concluded that control is a measure that maintains and/or modifies risk.

In this case, we comply with the definition given in ISO/IEC 27005. We consider that the measures act either on vulnerabilities, thereby reducing the likelihood of the threat occurring or on the consequences (harm) that the realization of the threat could bring about, thereby mitigating them. For the sake of completeness, let us add that controls are not the only category of risk treatment. According to ISO/IEC 27005, risk can be accepted, shared with a third party, or eliminated entirely by removing the assets it affects, albeit with objectives it supports.

3.7. VISUALIZATION OF KEY TERMS OF CYBER AND INFORMATION SECURITY

Based on the characteristics of the six concepts described above, the authors present a simplified conceptual model that graphically depicts the interaction of the key concepts and entities in the field of basic risk management, and consequently cyber and information security management. In addition to the conceptual model, a basic example is presented based on the terminology discussed.

The conceptual model in Figure 1 describes the entities and their relationship cardinalities using a so-called Crow's foot notation. This notation allows for the description of one-to-one, one-to-many (many-to-one), and many-to-many relationships. The conceptual model and the relationships are supposed to be read as follows (the list is not complete):

- Objective is supported by one or more assets.
- Asset supports one or more objectives. (Otherwise, it would not be an asset.)
- Event is a manifestation of exactly one threat (eventuality). (And vice versa.)
- Threat causes one or more instances of harm (negative consequences). (Otherwise, it would not be considered a threat.)
- An instance of harm harms exactly one asset. (This means that an instance of harm is always scoped to a particular asset.)
- Control treats zero or more vulnerabilities.

- Control treats zero or more instances of harm.
- Risk instance is informed by exactly one threat.
- Risk instance is informed by exactly one harm instance.

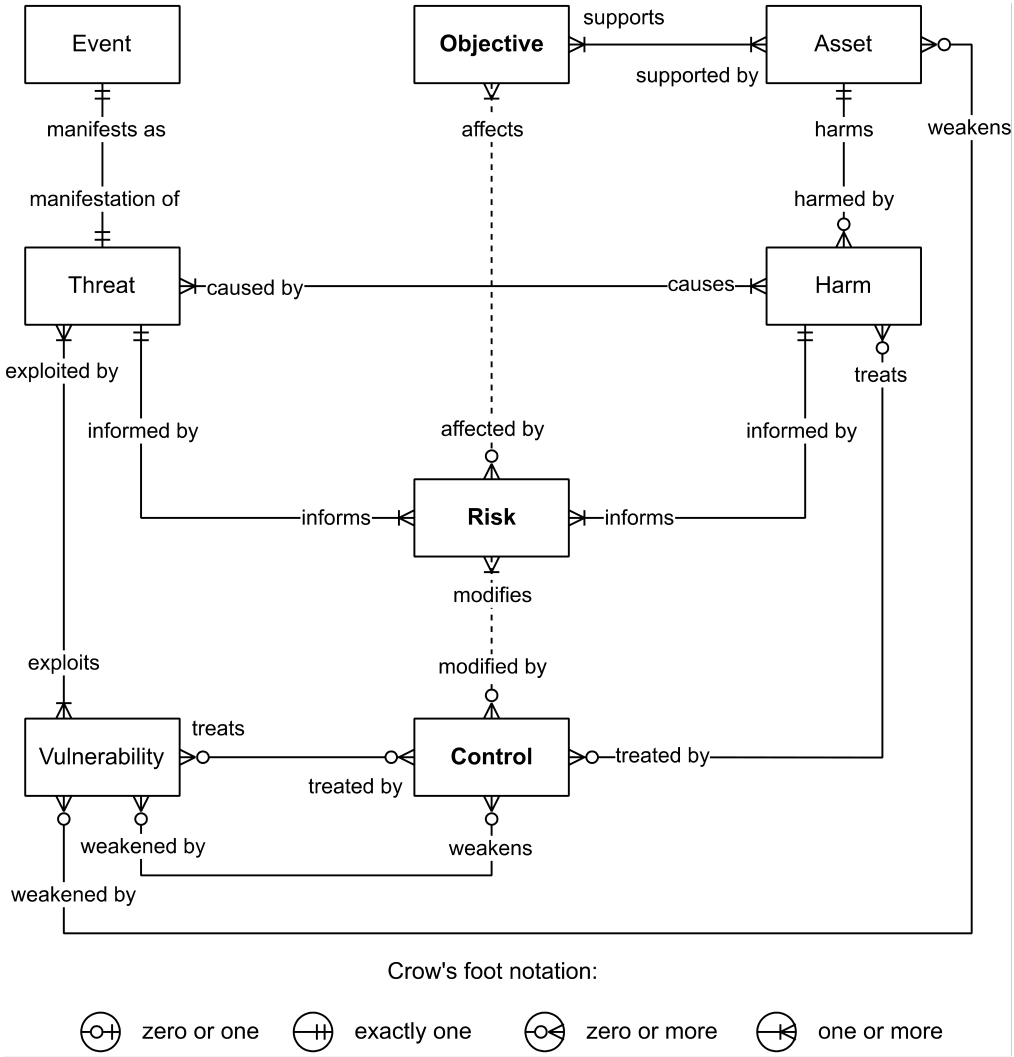

Figure 1: Conceptual model

The conceptual model can be explained by a relatively simple example:
Objective: Living in a house.

Asset: House of straw.
Threat: Structural damage due to strong wind.
Vulnerability: Straw is an extremely light material.
Harm: The house being destroyed (destruction).
Risk to asset: House being blown away (destroyed) by a strong wind.
Risk to the objective: Having nowhere to live.
Threat actor: The Wolf.
Event: The Wolf blew once.
Consequences: House was blown away.
Control (treating vulnerability): Use of better building materials, e.g., sticks or bricks.
Control (treating harm): Having plenty of straw to build a new house.
Risk treatment (avoiding risk): Not wanting to live in a house.
Risk treatment (removing the source of risk): Getting rid of the Wolf.
If this fairy tale story is applied to the field of cybersecurity, it could be demonstrated as follows:
Objective: Maintaining a good reputation among customers concerning data protection.
Asset: List of customers with personal details.
Threat
Threat: Access to data on lost storage medium.
Vulnerability: No encryption on storage media.
Harm: Disclosure of a list of customers with personal details (information disclosure).
Risk to the asset: Disclosure of a list of customers with personal details due to the access to data on lost storage medium.
Risk to the objective: Loss of reputation due to information disclosure.
Threat actor: Random finder.
Event: Storage medium lost, then found and accessed; information publicly disclosed.
Consequences: Asset confidentiality lost. Reputation lost.
Control (treating vulnerability): Storage media encryption.
Risk treatment (avoiding risk): Do not use portable media.
Risk treatment (removing the source of risk): Not applicable.

4. CONCLUSION

Therefore, to successfully and effectively apply and implement cyber and information security, it is necessary to understand the basic principles and concepts used in this area. The present paper specifically focused on the

legislative and technical characteristics of the most commonly used cyber and information security terms that are often considered notoriety.

From the presented analysis it is clear that these terms can be interpreted quite differently in different situations by different actors. This can lead to their inappropriate or even incorrect use. This misuse can be highly misleading and may result in a misconfigured information and cybersecurity management system.

All technical and legal documents which have been used within the article work with terms that are not used doctrinally and uniformly. On the contrary, they are often used synonymously and are also often overused in situations where their use is inappropriate. This degree of linguistic creativity can be observed both at the international and, in particular, at the national level in the context of the transposition of EU legal norms into national legislation.

For this article, definitions based on ISO/IEC 27000, NIST, CISA, NIS 1, and NIS 2 have been used. In this article, the authors sought to highlight the ambiguity in the interpretation of key cyber and information security concepts, both within and outside the European Union. A secondary aim was to highlight the not-always-clear and unambiguous terminology used in the NIS2 framework.

The purpose of this article was to highlight the differences described above and to suggest a possible starting point that would provide a generally accepted framework for the terminology in question for technical, legal, and user professionals alike.

Based on the comparisons of both technical and legal standards and the subsequent presentation of the links between the key concepts of cybersecurity within the Conceptual Model, the authors present the following conclusions:

- An asset is anything that has value and contributes to the achievement of an organization's objectives.
- An event is an occurrence or change of a particular set of circumstances within a particular domain; it is something that has happened, or is contemplated as having happened in that domain. We refer to a potential event as an eventuality.
- The threat is an eventuality that can be expected to have negative consequences for the objective.
- Vulnerability can be concluded as a weakness of an asset or control that can be exploited by a threat.

- Risk can be understood as the effect of uncertainty, resulting from the lack of information related to the likelihood and consequences of an eventuality, on the objectives.
- Control is a measure that maintains and/or modifies risk.

The presented Conceptual Model represents the basic framework, to which further sub-relations can be added. The article and its conclusions can therefore be used in further unification of technical and legal terminology.

The authors are convinced that the analysis, comparisons, and findings presented can contribute to a better understanding of the whole issue of cyber and information security. They can also contribute to a better transposition of European legal standards into national legislation, especially by using sufficiently general, non-confusing terminology.

LIST OF REFERENCES

[1] Cichonski, P. et al. (2012) Computer Security Incident Handling Guide [online]. *NIST Special Publication (SP)*, 800-61 Rev. 2. Gaithersburg, MA: National Institute of Standards and Technology. Available from: doi: https://doi.org/10.6028/NIST.SP.800-61r2

[2] *Committee on National Security Systems (CNSS) Glossary* [online]. Available from: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf [Accessed 10 January 2023].

[3] Council Decision 92/242/EEC on the security of information systems.

[4] *Cyber-attacks have tripled in past year, says Ukraine's cybersecurity agency* [online]. The Guardian. Available from: https://www.theguardian.com/world/2023/jan/19/cyber-attacks-have-tripled-in-past-year-says-ukraine-cybersecurity-agency [Accessed 20 February 2023].

[5] *The Cybersecurity Strategy* [online]. European Commission. Available from: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy [Accessed 8 August 2023].

[6] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[7] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[8] Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce).

[9] Directive 2002/19/EC of the European Parliament and of the Council on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive).

[10] Directive 2008/114/EC of the European Parliament and of the Council on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[11] Directive 91/250/EEC of the European Parliament and of the Council on the legal protection of computer programs.

[12] *Explore Terms: A Glossary of Common Cybersecurity Words and Phrases* [online]. NICCS. Available from: https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary [Accessed 10 January 2023].

[13] *Glossary* [online]. ENISA. Available from: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary [Accessed 10 January 2023].

[14] Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. [online]. NIST Special Publication (SP) 800-37 Rev. 1 Gaithersburg, MA: National Institute of Standards and Technology 2019.

[15] *Guide for Conducting Risk Assessments: Information Security* [online]. NIST. Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [Accessed 10 January 2023].

[16] *Industroyer2: Industroyer reloaded* [online]. Eset. Available from: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ [Accessed 20 February 2023].

[17] ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary.

[18] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

[19] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls.

[20] ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

[21] Kolouch, J. and Bašta, P. *CyberSecurity*. Praha, 2019: CZ.NIC. ISBN 978-80-88168-31-7.

[22] Niblett, P., Etzion, O. (2012) *Event Processing in Action*. Manning. ISBN 9781638352624.

[23] Regulation 460/2004/EC of the European Parliament and of the Council establishing the European Network and Information Security Agency, as amended by Regulation 1007/2008.

[24] *Russia's war on Ukraine: Timeline of cyber-attacks* [online]. European Parliament. Available from: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549 [Accessed 20 February 2023].

[25] Solms, R.V., & Niekerk, J.F. (2013). *From information security to cyber security. Comput. Secur., 38, 97-102*.