# Cybersecurity as a New Type of Security and Its New Perception

Miroslav Tomšů
*Tomas Bata University in Zlín*
Faculty of Applied Informatics
Zlín, Czech Republic
tomsu@utb.cz

***Abstract*— Cybersecurity is critical to both Prosperity and Security. As our daily lives and economies have become increasingly dependent on digital technologies, we have become increasingly exposed to cyber threats. Cybersecurity incidents are increasingly diverse - both in terms of who is responsible and what they are trying to achieve. Unfair activities in cyberspace threaten our economies - and the very functioning of democracies, freedoms, and values. This article describes Cybersecurity as a relatively new and unexplored security field. The introduction deals with the definition of Cybersecurity and its relationship with Cybernetics. It describes the short-term - (for now), development of Computer Security with Information Technology Development. The research section deals with separating Cybersecurity as a wholly new - and sovereign field of Information Security. This is followed by a description of the "life" of a new type of Security and Cybersecurity and Standardisation Security Issues. The conclusory part deals with the cybersecurity interest and content area.**

***Keywords — Cybersecurity, Information Security, Computer Security, Security Issues.***

## I. Introduction

Information Technology increasingly processes more and more information - with great value. When we talk about Information Processing with regard to Information Technologies; we mean using these technologies to store, transmit, evaluate, and present information.

Ensuring Information Security and Cybersecurity Information Security and Cybersecurity itself is undoubtedly one of the critical challenges of current times. In line with electronic public administration developments in the Czech Republic, the threat of cyber-attacks is increasingly becoming a more topical issue - and attacks are also becoming more sophisticated on a yearly basis.

The phrase Information Security is quite commonly used today - but many people do not know what to imagine under this expression. This is an area dedicated to all Information Security - (whether in physical or virtual forms), throughout its existence. If we do not protect this information, it could be leaked and misused - which would cause various problems.

Recently, Information Security has often been discussed, and it is somehow forgotten that Cybersecurity issues also exist. But are Information Security and Cybersecurity the same? Can we put an equal=sign between them? Is one security a subset of the other …. or is there some form of inter-action between them?

Defining the Cybersecurity concept is very important - especially since many people mistakenly believe that this issue only concerns Information and Communication Technologies departments. However, it also applies to everyone who uses any ICT elements in everyday life. This misconception may increase cyberattack success likelihood [1].

## II. Cybersecurity Causes Definition

The definition of Cybersecurity – further only cybersecurity - can be a somewhat problematic. For many people, cybersecurity is an area that is de facto dealt with exclusively by information and communication technology departments. However, this is a misinterpretation since cybersecurity concerns every information and communication elements user. The Human Factor is the crucial player in cybersecurity.

Cybersecurity cannot be underestimated. This is an area that is - in itself, crucial for many individuals or organisations. This area should address this in a long-term and systematic way, and all life cycle sub-aspects should be maintained.

### *A. The Cybersecurity Concept*

If we focus on our Cybersecurity/cybersecurity concept, it is appropriate to proceed from the analysis of this phrase.

The word cybernetics - from the Greek κυβερνητικός (cybernētikós); defines a science that deals with the general principles of information management and transmission in machine systems, living organisms, and communities. It is based on the knowledge that some living organisms' processes can be described by equations, similar to the same functions in technical devices. In the modern sense, it appeared in many fields that were part of it - and then developed independently - Computer Science, Artificial Intelligence, or Neural Networks [2].

Cyberspace can be defined as an intangible, virtual, digital environment that enables the creation, processing, and exchange of data and information using electronic communication. If we understand the term cyberspace in a broader sense, it is possible to include cyberspace users themselves.

Many definitions exist of cybersecurity in professional publications; but there is no single general definition. Therefore, it can be defined as a set of measures, means, rules, and mechanisms to limit threats to a reference object / digital asset.

The Merriam-Webster Dictionary states: Cybersecurity is a set of measures taken to protect a computer system from unauthorised access or attack [3].

The Oxford Dictionary states that cybersecurity is a state of protection against criminal or unauthorized electronic data. Cybersecurity must then, include the measures that need to be taken to achieve this [4].

Cybersecurity is also defined in the National Cyber Security Strategy of the Czech Republic for the 2015 - 2020 period. This strategy states that: "Cybersecurity is a set of organisational, political, legal, technical and educational measures and tools aimed at ensuring the secure, protected and resilient cyberspace in the Czech Republic; for both public and private sector entities, and for the general Czech public [5]."

Another definition of cybersecurity can be found - for example, in the European Agency's ENISA definition of Cybersecurity - Gaps and overlaps in standardisation: "Cybersecurity refers to cybersecurity, where cyberspace itself refers to a set of links between networks, and the very set of objects whose interfaces allow their remote control, remote access to data, or their involvement in management actions within cyberspace. Cybersecurity will include a paradigm of the CIA triad for relationships and objects within cyberspace, at the same time, this paradigm will be expanded to ensure the protection of the privacy of entities (individuals and legal entities) and resilience [6]."

In view of the above disagreement in opinions, we can present our definition, an analysis of several definitions and also based on their own experiences:

Cybersecurity is a set of measures, rules and mechanisms to ensure protection in the digital environment and beyond against unauthorised access, misuse or attack.

From the above inconsistencies in opinions, we can present our definition, created by examining previous definitions based on their own experience.

Cybersecurity is a set of measures, rules and mechanisms to ensure protection in the digital environment and beyond against unauthorised access, misuse or attack.

By the very nature of the meaning of the words, the concept of cybersecurity has been rather unhappily defined. More precisely - it is about protecting the Digital Environment, i.e., it should be about Digital Security.

## III. Cybersecurity Historical Development and Aspects

Many people assume that cybersecurity is a new sector that has relatively evolved over the last decade. Information security is created, along with the information needing protection. Specific information protection mechanisms - especially in the form of plaintext into encrypted conversion - began to emerge in antiquity in the form of cryptological cyphers.

The term "Cybersecurity" has been used for almost twenty years - since 2000, (and cybersecurity) used to describe all ways to protect assets in digital form. However, the environment has changed a lot during that time. Cybersecurity is still subject to constant and very dynamic development. An example can be the very focus of cybersecurity, which has evolved from an originally exclusively technical discipline into a strategic concept that has penetrated various areas of human life - not excluding Law fields.

Although cybernetics may seem related to cybersecurity; it is not. Cybernetics is a discipline that deals with management principles. At the same time, cybersecurity is more about digital security and does not address management processes; but its subject is digital space protection [7].

### *A. Cyber (Computer) Security in the 70s and 80s*

During the 1970s, the first symmetric (private key) encryption algorithms emerged as the DES (Data Encryption Standard), later replaced by the AES (Advanced Encryption Standard). Symmetric cryptography works with only one key, which is used to encrypt and decrypt text [8].

The origin of the field of information security dates back to the 1980s when the area was still called computer security, and it was mainly the security of computer networks. At this time, articles on this topic are also beginning to be published in professional periodicals [9].

### *B. The Standard for Cybersecurity in the USA*

As computers and systems became more and more advanced, experts worldwide were looking for ways to standardize aspects of computer systems. TCSEC (Trusted Computer Evaluation Criteria) was issued in 1983 - the first standard for cybersecurity. He described general safety requirements according to specific parts according to safety. It was created for the military environment, focused on the confidentiality of information.

In September of that year, the Massachusetts Institute of Technology (MIT) granted U.S. Patent 4,405,829 for a cryptographic communications system called RSA. Interestingly, this was the very first patent - whereas cryptography is a crucial part of cybersecurity strategies [10].

### *C. The Standard for Cybersecurity in Europe*

Before long, the first criteria in Europe already appeared in 1991. It was an ITSEC (Information Technology Security Evaluation Criteria). The standard has been adopted in France, Germany, England and the Netherlands. It included seven classes of warranties and defined another ten levels of functionality. It was designed in general and covered the requirements of integrity and availability of information [11].

### *D. Globalization*

Globalization or the interconnection of the world has also affected standards. The harmonization of TCSEC, ITSEC and the Canadian CTCPEC standard has created state-of-the-art CC (Creative Commons) criteria. The ISO International Standards Office has adopted these criteria as EAL1 to EAL7. The standards were subsequently translated and adopted into Czech technical standards under the designation ČSN ISO / IEC [11].

### *E. Computer Security in the Czechoslovak Republic since the 1980s*

The absence of factual sources makes it difficult to study the history of computer security in Czechoslovakia. It primarily related to the protection of classified information. In diplomatic relations, encryption means were used, such as the SA-1 encryption machine (designed by specialists from the Interior Ministry).

The number of cybercrime cases was negligible, only a limited number of people knew about it. The first case identified was the sabotage of causing malfunctions in the Pension Office's computer. However, the means used was a rarity - women's nylon underwear, causing electrostatic discharges, interfering with the computer's sensitive electronics.

The second half of the 1980s is more important in terms of computer security. Computer systems protection aspects articles began to appear in periodicals like Mechanization and Automation and Information Systems.

The rise of computer viruses has only driven a greater interest in computer security. Since 1985, informal specialist groups have been gradually formed outside the power departments. They thus created a precondition for the creation of security products and then also for specialized companies [11].

### F. *Computer Security in the Czech Republic in the 1990s*

Social changes in 1989 brought an acceleration in the information security field. Tuition of cryptography at universities began. The Criminalistics Institute in Prague established the first Cybercrime Department in 1992, Act No. 256/1992 Coll., On the protection of personal data in information systems, was adopted. The association of those interested in information security began, and - in 1993, they founded the Association of Companies for Data and Information Protection - (AFOI). A year later, the Group of Cryptology Union of Czech Mathematicians and Physicists International - (GCUCMP), was established. A branch of the international Information System Audit and Control Association (ISACA) organisation was also founded. The first international CISE - (Certified Information System Auditor), certificates began to be issued.

The first professional conferences held in the Czech Republic include "Pragocrypt" in 1996 and "Eurocrypt" in 1999. Articles dealing with information security began to appear to an increased extent in professional journals. At the end of 1996, the professional magazine Data Security Management started to be published, and in 1999, the electronic magazine Crypto-World was launched. With the year 2005 came a new concept of information security standardization [11].

## IV. The Emergence of Cybersecurity

The very definition of cybersecurity as a new security discipline has led to the rapid development of information and communication technologies. It is not possible to precisely date the emergence of cybersecurity; it is a gradual and logical separation of information security into cyberspace. However, this is sometimes incorrectly dated to 2014 - when the Cyber Security Act was approved, but its history goes back a long way. The Cyber Security Act Approval only complements the specifics necessary to denominate a new type of security [12].

### A. *Relationship between Information and Cybersecurity*

In most cases, it happens that information security and cybersecurity are considered synonymous. However, these are different terms that cannot be confused because of the various protection subject matters. We protect information but in other forms.

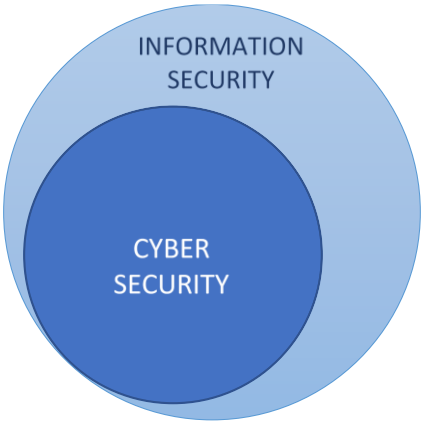

Fig. 1. Definition of Cybersecurity within Information Security

### B. *Cybersecurity Allocation Specifics*

Creating a new type of security is preceded by incentives that determine the need to define a new kind of protection. In the case of cybersecurity … these were emerging security issues and their institutionalisation [13].

Ensuring security is enforced by many tools, like:

- Legislation - (Act No. 181/2014 Coll. on Cybersecurity, Decree No. 316/2014 Coll. on Cybersecurity)
- Strategy - (National Cyber Security Strategy of the Czech Republic)
- Authorities - (National Office for Cyber and Information Security - NUKIB, established in 2017)
- Technology Management - (Information Security Management System - ISMS)
- Assurance and Enforcement Methods

Cybersecurity Tools are primarily associated with the state's critical infrastructure; but this does not change the need to apply cybersecurity to other organisations - in all sectors [14].

### C. *Detaching Cybersecurity*

The separation of cybersecurity as a separate field of security should occur through logical reasoning and gradual development. This development consists of the emergence of new asset protection specifics - software, databases, etc. The Computer Dictionary, (1993), defines "Information security is the protection of information in all its forms… [7]". It can therefore be assumed that this also includes information in digital form. However, the development of digital threats forces organisations to take measures and processes to protect these assets to such an extent that de-facto Information Security has become cybersecurity as a new field. With its standards set to address this specific - (digital) group of security issues; cybersecurity meets the exclusion aspects as a new type of security [15, 16]. By separating cybersecurity from information security, we can focus on cybersecurity and administrative security - and devote more attention to by describing it in detail.

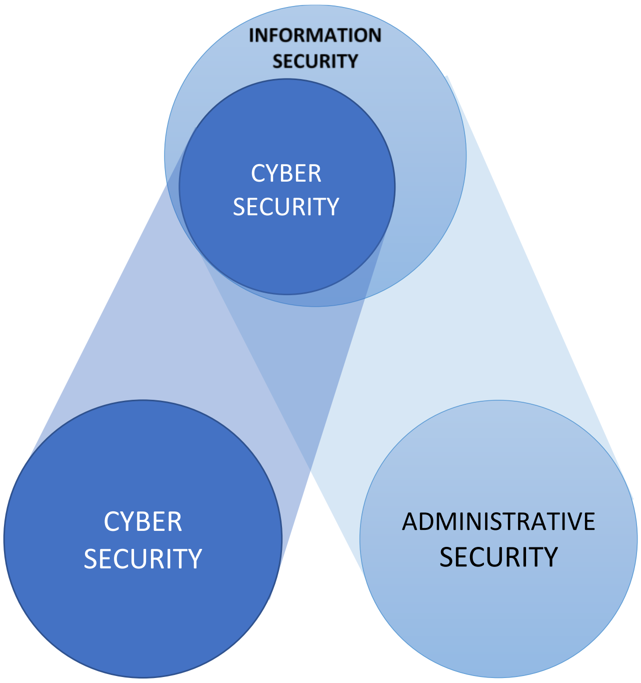

Fig. 2. Separating Cybersecurity from Information Security.

### D. Administrative Security

Administrative Security is a concept introduced by law. However, we are aware of all procedures and processes, and it can naturally be separated from information security as a particular type of security.

### E. Administrative Security "de lege lata"

Administrative Security is addressed by Decree No. 529/2005 Coll., on Administrative Security and Classified Information Register. The Decree defines it as "a system of measures in the creation, receipt, registration, processing, dispatch, transport, transmission, storage, disposal, archiving, or other handling of classified information." It deals primarily with the protection of classified information and is one of the basic types of protection. According to Act No. 412/2005 Coll., classified information on the Protection of Classified Information and Security Competence, as amended:

The Act on the Protection of Classified Information defines classified information as information in any form recorded on any medium marked per this Act, the disclosure or misuse of which may cause harm to the Czech Republic or maybe disadvantageous to this interest, and which is listed in the list of classified information [17].

Although legislation defines the resolution of security problems and stipulates their sanctions, there is an unresolved place in organisations that do not work with classified information.

### F. Administrative Security "de lege ferenda"

However, we can logically look at administrative security - (if we do not consider the letter of the law) as a unique type of security. There should be procedural rules "in the creation, receipt, registration, processing, sending, transport, transmission, storage, shredding procedure, archiving, or any other handling, [17]" regardless of whether we work with classified information defined under Act No. 412/2005.

Administrative Security would thus become a new logically created set of measures, resolving a specific group of administration security problems, that would arise from the logical separation from information security, based on the needs of the organisation's file service practice.

## V. Information Security after Allocation

There are two variants after the transfer of administrative and cybersecurity that may occur. Due to each organisation's needs in which this process takes place, information security - due to its operation may adapt to another group of security problems or disappear altogether.

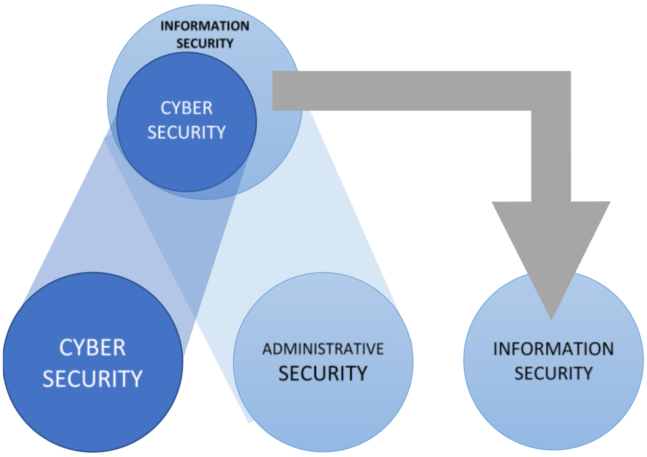

Fig. 3. Separation of Cybersecurity Together with the Application of Information Security in the Organisation.

## VI. The Subject of Cybersecurity

Cybersecurity is a technique for protecting cyberspace - (digital virtual environments), networks, programmes and data from unauthorised access - or attacks aimed at their misuse. These are also the main aspects and specifics for distinguishing cybersecurity from other security issues tied to the physical and material worlds.

### A. Cyber Environment Specifics

The cybernetic environment is specific not only for its subject - but also, by many other aspects:

- Intangible environment - cybernetic environment, virtualisation - (simulated computing environment), is the essence of its intangible assets; data is in the form of digital characters and codes that create a whole.
- Global accessibility - the environment is not limited by the organisation's boundaries, regions or states. Data stored in one country can be stored in remote storage on the other side of the world.
- Speed - the response to a command in a cyber environment is realised in the order of milliseconds to seconds. It all depends on the speed of the processor units - which are not slow at all.
- Anonymity - cyberspace users hide under their end stations' IP addresses, and it is never possible to determine whether it is a specific user.
- Change of identities - users work in a global environment, they can move very fast, they can change identities very quickly, but they can also disappear.

- Availability - The accessibility of the cyber environment is 24/365; restrictions that occur are only local and negligible.
- The asymmetry between "attackers" and "defenders" - unequal conditions for attackers and security managers, developers and IT professionals - the invisible environment emphasises greater security [18].

### B. *Cybersecurity Security Issues*

Most cybersecurity security issues occur in the digital environment - making them specific to that type of security. However, cyber problems effects are also reflected in the real environment – e.g., the loss and theft of information (assets), eavesdropping, data modification.

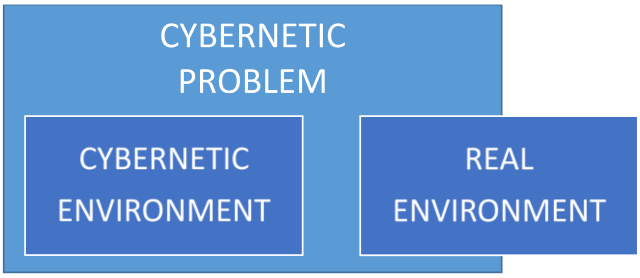

Fig. 4. Overlapping Cyber Problems into the Environment

Cybersecurity's security challenges are currently expanding according to digital space expansion and increasing interference in everyday life. The most common cyber problems can usually look like this:

- Phishing
- Trojans
- Botnets
- Ransomware
- Distributed Denial of Service (DDoS)
- Wiper Attacks
- Intellectual Property heft
- Money Theft
- Data Manipulation
- Data Destruction
- Spyware / Malware
- Man in The Middle
- Downloadable Files
- “Malvertising”
- Rogue Software
- Unrepaired software

### C. *Standardisation*

In cybersecurity history, digital security techniques have been developed to prevent or eliminate cybersecurity. Their creation was the storage of sensitive information on computers connected to the Internet, where they could be attacked.

The security techniques content is general outlines and specific organisation and institution techniques implementing cybersecurity. It is, therefore, possible to obtain certification for particular standards issued by an accredited certification body. The advantages of securing certification include - in particular, the possibility of attaining cyber insurance.

In the Czech Republic, cybersecurity standards at the national level are only taken over - and translated by the Office for Technical Standardisation, Metrology and State Testing and issued under the ČSN brand.

The most well-known standards include:

- ISO 27000 series - Issued gradually until 2005, international standards issued by the International Organization for Standardisation (ISO) and the International Electrotechnical Commission (IEC), focused on organisations' information security management. The certificate is suitable for organisations working with information - government, IT services, software companies, telecommunications operators, etc.
- Standard of Good Practice for Information Security - issued in 2011, the standard information security procedures - originally a private document for ISF - (Information Security Forum) members. The final form was released for sale to the general public. The latest version was published in 2013.
- NERC - Issued until 2006; originally - since 1956; standards developed by the North American Electric Reliability Corporation used to protect critical infrastructure and bulk electrical systems.
- NIST - Published since 1995, publications describe a broad overview of computer security and control areas (800-12), common security principles (800-14), IT security management (800-26), and risk approach (800-37).
- ISO 15408 - issued in 2005, develops the Common Criteria - allowing secure integration and testing.
- RFC 2196 - Issued in 1997, a memorandum published by the Internet Engineering Task Force on Developing Security Policies and Procedures for Information Systems Connected to the Internet; provides a general and broad overview of information security, including network security, incident response, or security policies.
- IASME - issued in 2010, a standard originating in the United Kingdom, provides criteria and certification for cybersecurity preparedness for small to medium-sized enterprises working with information [19].

## VII. Areas of Cybersecurity Interest and Content

Cybersecurity can be created or established by only three elements: The Human Factor, Processes and Technologies - and their interactions [1].

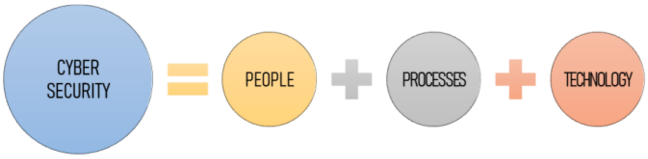

Fig. 5. Cybersecurity Attributes

In an organisation … people, processes, and technologies must effectively defend against cyber-attacks. Any system is as safe as its weakest link - (element).

### A. *People*

The Human Factor is crucial. As the primary and weakest link in the entire security system, users must adhere to data security principles. Above all, this involves selecting appropriate passwords, data access transfer to unauthorised persons, the monitoring of suspicious activities, low-security awareness, and the removal of classified information [20].

People in cybersecurity can be seen as:

- Cybersecurity creator/administrators.
- Cybersecurity rules recipients.
- Entities to be protected against cyber-attacks.
- Entities, educated in cybersecurity management and principles.
- Cybersecurity risks or threats to their creation and maintenance [1].

### B. *Processes*

The organisation must have a framework to deal with information leaks, integrity breaches, suppression of service, or illegitimate use. Processes can also be understood as steps that the organisation's management take to ensure better cybersecurity - compliance with standards and legislation, staff training. Techniques are also activities needed for usable human's technology [1].

Given the current period, it is possible to monitor these processes:

- Asset and Risk Management
- ICT Application Implementation
- User and Role Management
- Authorisation and Authentication
- Maintenance - Systems and Services updates
- Plans and Services Security Testing
- Cybersecurity Audits
- Anomaly or Cyber-attack Detection
- Cyber-attack or other Incident Responses
- Training and Education [1]

### C. *Technology*

Technology is essential for an organisation to have the security tools needed to protect against cyber-Frequent attacks. Three main entities must be protected: end-devices - computers, smart devices and routers; networks and clouds [1].

Commonly used technologies to protect these entities include:

- Detection Systems
- Central User and Administration Roles
- Centralised Information Classification Management
- Malicious Code Protection
- Individual Elements Activities Recording Technology - (log-in systems)
- Active and Offline Backup Systems
- Network Security Management [1].

## Discussion

The division of information and cybersecurity into two equal types of security undoubtedly leads to each of them focusing more on their methods, mechanisms, and processes to ensure better specific objectives security. This division should not lead to more bureaucracy through compliance with laws and regulations - but better applicability in organisations. Of course, there may be problems with applying different security types, and individual organisations will not be clear about which kind of security is a priority for them.

Organisations should work with specialists to further raise awareness of plans and organisations dedicated to securing their infrastructure. There should always be a plan to respond to cyberattacks, the management role - who are the contact persons for the sector at each level? How entities share information in an emergency. Under no circumstances should information or cybersecurity be prioritised, or one downplayed and the other prioritised! Both types of security need to be applied evenly and effectively in an organisation according to its needs.

## Conclusion

In recent years, tremendous changes and progress have been made in developing Information and Communication tools. Information and Communication Technologies have become our everyday companions and also - indispensable accessories for many of our activities. They expand trade, entrepreneurship, contacts with loved ones, or control of their finances.

A wide range of research methods and comparative approaches needs to be used to provide primary data on the incidence and dangers of different types of cybercrime. Research into the effectiveness of new legislation, policy strategies, and prosecution through case analysis and attrition studies is essential.

Research must not be limited to the police or judicial data, and these sources should often be more specific and uniform. Areas that require research most urgently include victim-offender behaviour and monitoring legislative developments and law enforcement around the world.

The Information and Cybersecurity Strategy should be evidence-based and rigorously evaluated to ensure efficiency and effectiveness.

Therefore, joint and coordinated efforts should be made at the international level to provide practical research funding mechanisms and reduce many emerging cybercrime types. However, it is equally essential to ensure that research is internationally coordinated, and that its results are widely available.

## ACKNOWLEDGMENT

This work was supported by Grant Project IGA/FAI/2021/003 “SW Population Protection and Soft Target Support” - resolved in 2021.

## REFERENCES

[1] J. Kolouch and P. Basta, CyberSecurity, Prague: CZ.NIC, z.s.p.o., 2019.

[2] J. Rejzek, Czech Etymological Dictionary. 3rd ed. Prague: Leda, 2015.

[3] “Cybersecurity,” Jan. 6, 2021. Accessed on: Jan. 22, 2021. [Online]. Available: https://www.merriam-webster.com/dictionary/cybersecurity

[4] “Cybersecurity.” Accessed on: Jan. 29, 2021. [Online]. Available: https://en.oxforddictionaries.com/definition/cybersecurity

[5] National Cyber and Information Security Agency, *National Cyber Security Strategy of the Czech Republic for the period from 2015 to 2020*, Mar. 12, 2015. Accessed on: Jan. 25, 2021. [Online]. Available: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf, p. 5.

[6] European Union Agency for Cybersecurity, *Definition of Cybersecurity - Gaps and overlaps in standardisation*, ENISA, Heraklion, Greece, Dec. 2015. Accessed on: Jan. 29, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/definition-of-cybersecurity, p. 30.

[7] P. G. Aitken, Dictionary of Computer Technology: Interpretation of Standard Terms for Science, Eeducation and Business. Prague: Plus, 1993.

[8] J. M. Carrol, Computer Security. 3rd ed., Oxford: Butterworth Publishers, 1987.

[9] L. Dobda, Data Protection in Information Systems. Prague: Grada, 1998.

[10] J. Janecek, Revealed Secrets of the Encryption Keys of the Past: Hand Ciphers. Prague: Our Army, 1994.

[11] M. Drastich, Information Security Management System. Prague: Grada, 2011.

[12] M. Hromada, P. Hruza, J. Kaderka, O. Lunacek, M. Necas, B. Ptacek, L. Skorusa and R. Slozil, Cybersecurity: Theory and Practice. Prague: Powerprint, 2015.

[13] National Cyber and Information Security Agency, *The Process of Determining the Basic Service Operator and the Basic Service Information System According to the Cybersecurity Act and the Decree on Criteria for Determining Basic Service Operators*, Aug. 7, 2018. Accessed on: Feb. 5, 2021. [Online]. Available: https://www.govcert.cz/download/kii-vis/Schema_rozhodovani_PZS_v2.1.pdf, p. 1.

[14] Security Information Service, *Annual Report of the Security Information Service for 2017*. Accessed on: Feb. 6, 2021. [Online]. Available: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2017-vz-cz.pdf, p. 15 et seq.

[15] L. Lukas, “Security Theory and Typology of Types of Security,” in Crisis Management in a Specific Environment. Zilina: Faculty of Safety Engineering UNIZA, 2016, pp. 324-331.

[16] B. Buzan, O. Waever and J. de Wilde, Security: A New Framework for Analysis. Brno: Center for Strategic Studies, 2005.

[17] Act No. 412/2005 Coll., on the protection of classified information and security clearance, as amended.

[18] V. Jirovsky, Cybercrime: Not Just About Hacking, Cracking, Viruses, and Trojans Without Secrets. Prague: Grada, 2007.

[19] Act No. 181/2014 Coll. on Cyber Security and Amendments to Related Laws.

[20] B Schneider, Secrets and Lies: Digital Security in a Networked World. 15th ed. Indianapolis, Indiana: John Wiley & Sons, Inc., 2015.