CYBERSECURITY AUTHORITIES AND RELATED POLICIES IN THE EU AND HUNGARY

Tamás Szádeczky[1]

DOI: 10.24989/ocg.v331.24

Abstract
Parallel with the evolving of cyber conflicts, the need for appropriate handling of the public administration tasks also appeared. Governmental tasks were necessary, which includes defense (military), diplomatic, law enforcement and public administrative factors also.

This paper shows an analysis of the institutional background of cybersecurity administration in the European Union and Hungary in parallel. This includes the regulations about ENISA, the European Union Cybersecurity Agency, the Hungarian cybersecurity authorities, and the cybersecurity strategies for both entities, namely Regulation (EC) No 460/2004, Cybersecurity Strategy of the European Union of 2017, Regulation (EU) 526/2013, COM/2016/0410 final, 2017/0225 (COD) Proposal, Hungarian Government decree no. 223/2009, Government Decision no. 1139/2013, Act L of 2013, and Government Decree 187/2015.

The research has been supported by the ÚNKP-17-4-III-NKE-26 New National Excellence Program of the Ministry of Human Capacities.

Keywords: *cyber strategy; information security legislation; incident response*

1. Introduction

The word cybersecurity seems to be a bit overused nowadays, but as other researchers already shown, it is different from the "classical" term information security. In both terms, information-based assets stored or transmitted using information and communication technologies (ICT) is included. But information security also includes paper-based information. The term cybersecurity includes non-information based assets (e.g., a high-voltage substation) that are vulnerable to threats via ICT. This is similar to the interdependency between critical infrastructure elements).[2] The new model of cybersecurity needs a different approach to security organization: the classical security models have to be revised.[3]

The importance of cybersecurity is well-known and often communicated by decision makers. However, the implementation, preparedness, and knowledge have deficiencies. This might happen because of lack of knowledge, resources or experience.

[1] Ph.D., senior lecturer, National University of Public Service, Faculty of Science of Public Governance and Administration, Institute of E-Government, 1083 Budapest, Üllői út 82., Hungary, szadeczky.tamas@uni-nke.hu
[2] Solms, Rossouw von, Niekerk, Johan van, From information security to cyber security, Computers & Security, Volume 38, 2013, Pages 97-102, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2013.04.004.
[3] Leuprecht, Christian, Skillicorn, David B., Tait, Victoria E., Beyond the Castle Model of cyber-risk and cyber-security, Government Information Quarterly, Volume 33, Issue 2, April 2016, Pages 250-257 doi:10.1016/j.giq.2016.01.012

Technology development, as we described above, made local system security improvements indispensable.[4] In case of e-government systems, a higher level of the problem also exists: attack against multiple systems or against a full infrastructure. This can take part of a conventional war, as cyberwar or may be an unconventional event, called cyberterrorist attack; they are all part of cybersecurity. Thus a major part of cybersecurity can be only handled with governmental or supranational level, with cybersecurity strategies,[5] legal regulation, and dedicated authorities.
Table 1 shows the changes in the EU and in Hungary parallelly, which will be detailed in this article.

Year	The European Union	Hungary
2004	Regulation on establishing ENISA	
2012		National Security Strategy
2013	EU Cybersecurity Strategy The new regulation on ENISA	National Cybersecurity Strategy Governmental Information Security Act
2016	NIS directive	
2017	Cybersecurity Act (proposal)	National Cybersecurity Strategy (change proposal according to NIS)

Table 1: Legal regulations about cybersecurity in the EU and Hungary

2. Cybersecurity strategy in the EU

Before forming any exact strategy, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency* came into force. The regulation established ENISA, with the following objectives:

- *The Agency shall enhance the capability of the Community, the Member States and, as a consequence, the business community to prevent, address and to respond to network and information security problems.*

- *The Agency shall provide assistance and deliver advice to the Commission and the Member States on issues related to network and information security falling within its competencies as set out in this Regulation.*

- *Building on national and Community efforts, the Agency shall develop a high level of expertise. The Agency shall use this expertise to stimulate broad cooperation between actors from the public and private sectors.*

[4] Szádeczky, Tamás. The role of technology. Auditing and certification in the field of data security. In.: Gergely László Szőke (ed.): Privacy in the Workplace. Data Protection Law and Self-regulation in Germany and Hungary, HVG-ORAC, Budapest 2012, pp. 311-337.
[5] James A. Lewis, National Perceptions of Cyber Threats, Strategic Analysis, 38:4, 2014, 566-576, doi:10.1080/09700161.2014.918445

- *The Agency shall assist the Commission, where called upon, in the technical preparatory work for updating and developing Community legislation in the field of network and information security.*

It is important to remark the verbs used: enhance, provide, develop, and update. They show us the aim to form a soft agency without policy-making power. The exact plans with ENISA were also unclear.[6]

The tasks aligned with the objectives above were the followings:

- collect appropriate information to analyze current and emerging risks
- provide advice to stakeholders
- enhance cooperation between different actors
- facilitate cooperation the Commission and the Member States
- contribute to awareness raising
- assist the Commission and the Member States in their dialogue with industry
- track the development of standards
- advise the Commission on research
- promote risk assessment activities,
- contribute to Community efforts to cooperate with third countries
- express its own conclusions independently,

As we see from the list above, the tasks are supportive functions. There are no regulatory, standardization or audit functions dedicated to ENISA. In contrast to the field of data protection, the European Data Protection Supervisor has authority to audit EU organizations.

The bodies of ENISA are the Management Board, the Executive Director, and the Permanent Stakeholders' Group.

The first official cybersecurity strategy in the European Union was formed with the Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union. It's the Open, Safe and Secure Cyberspace formed on the 7th February 2013.

The strategy defined five strategic priorities, which address the challenges:

[6] Hearn, J. (2003). Moving forward? Security & Privacy, 1(2), 70–71.

- Achieving cyber resilience
- Drastically reducing cybercrime
- Developing cyber defense policy and capabilities related to the Common Security and Defence Policy (CSDP)
- Develop the industrial and technological resources for cybersecurity
- Establish a coherent international cyberspace policy for the European Union and promote core EU values

In the first strategic priority, achieving cyber resilience, the need to modernize and strengthen ENISA was articulated.[7]

After nine years of ENISA's operation and providing nearly 300 publications, with focus topics incident- and risk management, critical infrastructure protection, trust services and computing cloud, a new regulation came into force. Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21st May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 has changed the objectives:

- The Agency shall develop and maintain a high level of expertise.
- The Agency shall assist the Union institutions, bodies, offices and agencies in developing policies in network and information security.
- The Agency shall assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to the proper functioning of the internal market.
- The Agency shall assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents.
- The Agency shall use its expertise to stimulate broad cooperation between actors from the public and private sectors.

The tasks were also changed according to the objectives:

- support the development of Union policy and law, by advising, providing preparatory work, analyzing

[7] Ruohonen, Jukka, Hyrynsalmi, Sami, Leppänen, Ville, An outlook on the institutional evolution of the European Union cyber security apparatus, Government Information Quarterly, Volume 33, Issue 4, October 2016, Pages 746-756 doi:10.1016/j.giq.2016.10.003

- support capability building by supporting the Member States, promoting voluntary cooperation, assisting by supporting the operation of a Computer Emergency Response Team (CERT) for them;

- supporting the raising of the level of capabilities of national/governmental and Union CERTs, including by promoting dialogue and exchange of information, with a view to ensuring that, with regard to the state of the art, each CERT meets a common set of minimum capabilities and operates according to best practices;

- support voluntary cooperation

- cooperate with Union institutions, bodies, offices and agencies,

- contribute to the Union's efforts to cooperate with third countries and international organizations

The most important change in the tasks was the establishment of CERT-EU,[8] as a new service, and also a part of Computer Security Incident Response Teams (CSIRT) network according to NIS directive.[9] Incident management became more important in the operation of ENISA with these changes than in 2004. The incident management theory and practice are very wide; they include the range from operational procedures to governmental response. Illustrative key topics are ISO/IEC 27035, ITIL-based incident response, forensics, and operation of CSIRTs.[10]

The only change in the organization was the staff's addition to the Executive Director, and the Management Board shall establish an Executive Board.

In 2016 the European Commission adopted the Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final. The document dealt with the making the most of NIS cooperation mechanisms and moving towards ENISA 2.0. The section also mentions European Cybercrime Centre (EC3) at Europol as a possible cooperation partner. The Commission is required to evaluate ENISA by 20 June 2018 but plans to do it earlier.

So that a future change is foreseeable with the 2017/0225 (COD) Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency," and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"). The voting is forecasted to June 2018. The objectives of ENISA changed slightly:

- *The Agency shall be a center of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers and the information it provides, the transparency of its operating procedures and methods of operation, and its diligence in carrying out its tasks.*

[8] Website of CERT-EU is accessible at https://cert.europa.eu/
[9] Directive (EU) 2016/1148 Article 12. Par. 2.
[10] Tondel, Inger Anne, Line, Maria B., Jaatun, Martin Gilje, Information security incident management: Current practice as reported in the literature, Computers & Security, Volume 45, September 2014, Pages 42-57 doi:10.1016/j.cose.2014.05.003

- *The Agency shall assist the Union institutions, agencies, and bodies, as well as the Member States, in developing and implementing policies related to cybersecurity.*

- *The Agency shall support capacity building and preparedness across the Union, by assisting the Union, Member States and public and private stakeholders in order to increase the protection of their network and information systems, develop skills and competencies in the field of cybersecurity, and achieve cyber resilience.*

- *The Agency shall promote cooperation and coordination at Union level among the Member States, Union institutions, agencies and bodies, and relevant stakeholders, including the private sector, on matters related to cybersecurity.*

- *The Agency shall increase cybersecurity capabilities at Union level in order to complement the action of Member States in preventing and responding to cyber threats, notably in the event of cross-border incidents.*

- *The Agency shall promote the use of certification, including by contributing to the establishment and maintenance of a cybersecurity certification framework at Union level in accordance with Title III of this Regulation, with a view to increasing transparency of cybersecurity assurance of ICT products and services and thus strengthen trust in the digital internal market.*

- *The Agency shall promote a high level of awareness of citizens and businesses on issues related to the cybersecurity.*

The tasks improved heavily: the task list consists of 60 elements, grouped into the following seven articles:

- Tasks relating to the development and implementation of Union policy and law

- Tasks relating to capacity building

- Tasks relating to operational cooperation at Union level

- Tasks relating to the market, cybersecurity certification, and standardization

- Tasks relating to knowledge, information and awareness raising

- Tasks relating to research and innovation

- Tasks relating to international cooperation

Furthermore, on 13 September 2017, the President of the European Commission, Jean Claude Juncker announced an implementation toolkit for the Network and Information Security Directive; and a report to ensure an effective response in case of cyber-attacks in the Member States.

3. Cybersecurity organization in Hungary

The first comprehensive security and defense policy system of Hungary after the political change in 1989 did not recognize cyber threats. Neither the National Assembly resolution no. 94/1998 (XII. 29.) on the security- and defense policy principles of Republic of Hungary, nor the Government resolution no. 2073/2004. (IV. 15.) on the National Security Strategy of the Republic of Hungary, nor the Government resolution no. 1009/2009. (I. 30.) on the National Military Strategy of the Republic of Hungary included cyber defense as an objective. According to these policies and strategies, the defense against cyber attacks was treated individually, even in the legal regulation.

Before the Act on Electronic Public Service (before 29 June 2009) there was no acts dealing with information security in public- or governmental networks.[11]

Only the following Government decrees regulated the field:

- 195/2005 (IX. 22) Government Decree on security, interoperability and uniform use of electronic administration systems
- 84/2007 (IV. 25) Government Decree on security requirements of the Central Electronic Service System and related systems
- 193/2005 (IX. 22) Government Decree on detailed rules for the electronic filing
- 194/2005 (IX. 22) Government Decree on requirements for electronic signatures and the associated certificates used in the administrative proceedings, as well as requirements for certification service providers issuing the certificates
- 182/2007 (VII. 10) on the regulation of the central electronic service provider system

These provided security rules sporadically to some systems, without any general framework.

As a result, we may say that relatively low awareness of the legislator and the business is observable in the usage of international IT security standards, despite its significance and the high risk in some areas. No obligations were found in acts of Hungarian Parliament for enforcement of standards in IT security. There have been built-in self-control procedures in some acts, but in practice, those procedures actually haven't worked efficiently.[12]

In 2009 a small change was commenced with the adoption of Act LX of 2009 on electronic public services. It has highlighted the requirement of security as a basic principle.

Organizations providing ICT based public services ensure the publicity of data of public interest (according to the Act on data protection and freedom of information) and protection of personal and any other data during the provision of services.[13]

---

[11] Dedinszky, Ferenc, Informatikai biztonsági elvárások (Information security requirements), MeH-EKK, Budapest, 2008, p. 4.
[12] Szádeczky, Tamás. Information Security - Strategy, Codification and Awareness. In: András Nemeslaki (Ed.): ICT Driven Public Service Innovation. Comparative Approach Focusing on Hungary. Budapest, 2014. pp. 109-122.
[13] Hungarian Act LX of 2009 on electronic public services

During the provision of services, particular attention must also be paid to the fulfillment of realization of information rights, protection of classified information, business secrets and other protected data groups. Service providers ensure IT security, including the integrity of electronic records, and applicability of the electronic signature technology. The legislator refers to the application of electronic signature technology and the importance of compliance with the relevant security requirements.

The use of electronic signatures, according to Act on electronic signature (hereinafter Eat.) can greatly assist in maintaining the integrity of data. However, a huge discrepancy is noticeable between theoretical principles and practice. Despite the above rules, electronic signatures are still not widely adopted and rarely used in such systems.

Service providers shall also ensure the operational continuity and enforcement of information system collaboration requirements. As we have shown in chapter 4 and chapter 5 interoperability, i.e., cooperation between the various systems has particular importance in the government information technology, as island-like systems have been developed, and over time the demand of integration increased fairly. The negative impact of island-like development is still being felt in the area of interoperation. The continuity of operation, as one of the main requirements for IT security, including disaster and business continuity planning, is an important feature for large government databases, where data loss could and would be catastrophic.

Data transmitted to the central system profiling (analysis of user habits, personal information and direct access to meaningful case data) is not allowed according to these regulations. Compliance is ensured with the central system operator by means of technical solution. Profiling, one of the most challenging privacy issue in recent years is declared to be prohibited by a principle in Act LX of 2009 on electronic public services, and the information system must ensure this technically (e.g., through Privacy by Design technologies).

Use of remote services required a face-to-face pre-registration or an equivalent measure and given that a significant number of electronic public services are administrative procedures, they need proper identification. Personal appearance and identification mean a registration in governmental offices or registration by electronic signature.

Authenticity, quality, operational security and confidentiality of the data processed in electronic public services operate under the Central System must comply with defined rules. Here the act refers to Government decree no. 223/2009 (X. 14) about the security of electronic public services. In that, the requirements and procedures were determined in sections from 11 to 32. Requirements set out in the Act are detailed in the following regulations:

- Government Decree 223/2009 (X. 14) on the security of electronic public services
- Government Decree 224/2009 (X. 14) on the central electronic system service’s recipient identification and authentication services
- Government Decree 225/2009 (X. 14) on electronic public services and their use
- Government Decree 78/2010 (III. 25) on requirements of electronic signatures in administration and certain rules for electronic communication

There was a bill on information security in 2009, which never came to force, but had a remarkable impact on the area.[14] The proposal was a draft legislation framework, a so-called lex specialis.
The bill's scope was all IT systems and services in the Republic of Hungary, including private computers. It would have been applied to the operators and users, also.

According to this information systems are to be divided into 5 separate security level. One of the factors of the grouping was storage of personal data. The groups were the followings:

- Level 1: home computer networks and individual computers connected to the Internet
- Level 2: information systems used by every legal relationship between employer and employee, internal IT network, limited internal access non-public electronic communications services or internal network or individual computer capable of using public electronic services
- Level 3: any public electronic services that don't handle, store, process or transfer personally identifiable information, including anonymous registration services
- Level 4: organizations providing public electronic services, application service provider and it's public electronic services, regardless of personal data processing; any public electronic services that handle, store, process or transfer personally identifiable information
- Level 5: critical infrastructure sector's computer system, closed-circuit, and public electronic network or services and information technology

One of the most interesting questions is the mandatory audit required at level 4-5 as a mean of control. According to the original intention, this control would have been conducted by audit firms which are accredited previously by the National Accreditation Body for Certification Activity. Creators of the legislation could not specify whether that responsibility belongs to management systems or product certification.

Most importantly, the social impact of the law would have been significant, at least because of its wide scope. Critics had said there was lack of audit control in level 1 to 3, which made it a redundant regulation. In contrast to that, the legislation could have set the level of security requirements under other laws, because of its lex specialis character. For example, in Criminal Code Section 423 *adequate protection* is required in the case of hacking, but it was not defined earlier. The new law might have given meaningful content to it, and increasing legal certainty.

Government Decision no. 1035/2012 (II.21.) on Hungary's National Security Strategy required the strengthening of the security of electronic information systems to enhance the protection of critical national information infrastructure, and the development of the adequate cyber defense.

Stemming from this statement of the National Security Strategy, the Government adopted the Government Decision no. 1139/2013 (III. 21.) on Hungary's National Cybersecurity Strategy. The main objective therein:

- Establish incident reporting mechanisms
- Establish an incident response capability

[14] MeH, Draft of act on information security, 2009.

- Engage in international cooperation
- Strengthen training and educational programs
- Establish baseline security requirements
- Organize cyber security exercises
- Critical Information Infrastructure Protection
- Develop national cyber contingency plans
- Establish an institutionalized form of cooperation between public agencies

The legislator took the view that recently experienced cyber wars worldwide justified the coding of a modern Hungarian Information Security Act and on 25th April 2013 was a huge milestone for the administrative control of information, when Act L of 2013 on the electronic security of state and local government organizations was published.

The scope of the act, despite its title and scope definition in Section 2, is significantly wider as it seems to be,[15] mainly because of the following extensions: data processors of national data assets, European critical infrastructure system elements, national critical infrastructure system elements, as defined by law. These bodies can significantly extend the scope (even with private companies), so typically the public utility providers, electronic communications services, financial organizations could be included. An itemized list has not been published at the time of writing this manuscript. The law prescribes the essential items known as CIA triad (confidentiality, integrity, and availability) in information security field.

The Act requires the integrity and the availability of information systems in a closed, complete, consistent way, proportionate to the risks for the electronic system and components. It is important to explicitly include the security control implementation's proportionality to risks and use of risk assessment in the state information security requirements, because security measures are typically implemented in an ad hoc manner, to minimize security budgets.

In order to protect electronic information systems and data, proportionally to the risks, the Act states that the electronic information systems must be allocated to particular security classes. This classification is based on confidentiality, integrity and availability properties on a scale of 1 to 5, where 5 is the highest security level. From this section of the Act it seems that each part of CIA factors has to be evaluated separately, but from other parts of the Act, we don't find this distinction.

Although the security classification depends primarily on the security classification of information, the law, in contrast to the earlier bill, does not specify what minimal security controls should be applied to data. In contrast, in Section 9 (2) it determines the minimum security level classification for a variety of organizations. This probably will have the consequence that the security needs of data will not be evaluated. Instead, it will be adjusted to the security levels according to the minimum-list since public sector tries to spend as few as possible on security. According to the Act

[15] Muha, L., Krasznay, Cs., Kibervédelem Magyarországon: áldás vagy átok? (Cyber defence in Hungary: Bless or curse?), HWSW ONLINE, 2013: Paper 5026.

Section 7 para 5, in *exceptional circumstances*, the manager of the organization may set a lower security class, which is another easier way to avoid spending on security. The only thing that can stop this expected downward bidding, the strictness of National Electronic Information Security Authority, based on Section 9 Para 4. The authority is formed by Act Section 14 Para 1.
The minimum grades in the Act per organizations according to Section 9 Para 2:

- Level 1: no organizations (no requirements at this level)
- Level 2: Office of the President, Office of the National Assembly, the Constitutional Court 's Office, Office of the Commissioner for Fundamental Rights, local and national self-governmental bodies, the administrative authority associations
- Level 3: central state administration bodies, the National Judicial Office, courts, prosecutors' offices, the State Audit Office, National Bank of Hungary, the capital city and county government offices
- Level 4: Hungarian Defense Forces
- Level 5: data processors of national data assets, European critical infrastructure system elements, national critical infrastructure system elements, as defined by law

As we mentioned earlier, the law does not define what these security levels are, or how should the classification be conducted and what the detailed rules for the levels are.

According to Section 11 Para 1 (c), the head of the organization is obliged to appoint a person in charge of the electronic information system security, who is responsible for tasks related to the protection of electronic information systems. The list of tasks includes responsibilities of a conventional chief information security officer (CISO). Its name and definition are suggesting that this person exempt the head of the organization and its employees from their security-related task, but this shouldn’t be the case.

The Act set up the National Electronic Information Security Authority under the Ministry of National Development. As a specialized authority, National Security Authority is involved in their activities with forensic log analysis and vulnerability testing. The existing Government Computer Emergency Response Team (GovCERT) responsibilities have been migrated to the Special Service for National Security. According to Section 23, the National University of Public Service developed training for those responsible for the security of electronic information systems and staff organizations.

After changes of political forces in the government, the topic of cybersecurity was handed over to Ministry of Interior with the Government Decree 187/2015. (VII. 13.). Thus the National Cyber Defense Institute formed in the Special Service for National Security with the following elements:

- administration by National Electronic Information Security Authority
- incident management and response by GovCERT-Hungary
- forensic log analysis and vulnerability testing by National Security Authority

This is also the actual setup as of January 2018. National Cyber Defense Institute is planned to be competent national authority according to NIS.[16] There are four designated CSIRTs:[17] LRLIBEK for critical infrastructures, operated by National Directorate General for Disaster Management, Ministry of the Interior, MILCERT operated by the Military National Security Service, Hun-CERT the Hungarian Computer Emergency Response Team for Council of Internet Service Providers operated by the Hungarian Academy of Sciences Institute for Computer Science and Control, and NIIF-CSIRT, which is the Computer Security Incidents Response Team of NIIF/HUNGARNET, the Internet provider of universities, higher education institutes, some secondary schools, academical research organisations and non-profit institutions in Hungary operated by National Information Infrastructure Development Institute.

4. Conclusion

ENISA was established in 2004 as a consultative body. Both the EU and the Hungarian Cybersecurity Strategy was accepted in 2013. The strategies implied changes in the treatment of cybersecurity topic at the higher level. The objectives and tasks of ENISA have been changed, and the Hungarian authority was formed that year. The next hop was the NIS directive and its implementation in the member states' law, which also provides reinforcement to EU legislation to improve ENISA.

One of the main objectives and tasks both for ENISA and in the Hungarian regulation is the training. Even in the private sector, there is a huge need for well-trained IT personnel. The required level of training is much higher in the cybersecurity, and also real-life laboratories shall be used for such training.[18]

Another aspect of cybersecurity is the military or cyber warfare field. Many EU members, as well as Hungary, is a NATO member, which shapes our defense politics more than the EU Common Security and Defense Policy. NATO recognized cyberspace as a 'Domain of Operations' at Warsaw Summit in 8-9 July 2016. In fact, there are also no elements, which are directly applicable at the member level. But the thing that cyberspace became the fifth domain of operation, and the requirement that all military operations shall include operations will have a positive effect on the defense.

More changes happened in the previous years in the European legislation, and therefore preparedness to cybersecurity risk is much better nowadays, but we are lagged behind the United States of America and behind China.[19] Thus there is a long way to go.

[16] Article 8 of Directive (EU) 2016/1148

[17] According to Article 8 of Directive (EU) 2016/1148

[18] Dominguez, Manuel, Prada, Miguel A., Reguera, Perfecto, Fuertes, Juan J., Alonso, Serafin, Moran, Antonio, Cybersecurity training in control systems
using real equipment, IFAC PapersOnLine 50-1 (2017) 12179–12184, doi:10.1016/j.ifacol.2017.08.2151

[19] Krzysztof Feliks Sliwinski, Moving beyond the European Union's Weakness as a Cyber-Security Agent, Contemporary Security Policy, 35:3, 2014, 468-486, doi:10.1080/13523260.2014.959261

5. References

[1] DEDINSZKY, F., Informatikai biztonsági elvárások (Information security requirements), MeH-EKK, Budapest, 2008, p. 4.

[2] DOMINGUEZ, M. et al., Cybersecurity training in control systems using real equipment, IFAC PapersOnLine 50-1 (2017) 12179–12184, doi:10.1016/j.ifacol.2017.08.2151

[3] HEARN, J. (2003). Moving forward? Security & Privacy, 1(2), 70–71.

[4] LEUPRECHT, C. et al., Beyond the Castle Model of cyber-risk and cyber-security, Government Information Quarterly, Volume 33, Issue 2, April 2016, Pages 250-257 doi:10.1016/j.giq.2016.01.012

[5] LEWIS, J. A., National Perceptions of Cyber Threats, Strategic Analysis, 38:4, 2014, 566-576, doi:10.1080/09700161.2014.918445

[6] MUHA, L., KRASZNAY, Cs., Kibervédelem Magyarországon: áldás vagy átok? (Cyber defence in Hungary: Bless or curse?), HWSW ONLINE, 2013: Paper 5026.

[7] RUOHONEN, J., HYRYNSALMI, S., LEPPÄNEN, V., An outlook on the institutional evolution of the European Union cyber security apparatus, Government Information Quarterly, Volume 33, Issue 4, October 2016, Pages 746-756 doi:10.1016/j.giq.2016.10.003

[8] SLIWINSKI K. F., Moving beyond the European Union's Weakness as a Cyber-Security Agent, Contemporary Security Policy, 35:3, 2014, 468-486, doi:10.1080/13523260.2014.959261

[9] SOLMS, R., NIEKERK, J., From information security to cyber security, Computers & Security, Volume 38, 2013, Pages 97-102, ISSN 0167-4048, doi:10.1016/j.cose.2013.04.004.

[10] SZÁDECZKY, T., Information Security - Strategy, Codification and Awareness. In: NEMESLAKI, A., (Ed.): ICT Driven Public Service Innovation. Comparative Approach Focusing on Hungary. Budapest, 2014. pp. 109-122.

[11] SZÁDECZKY, T., The role of technology. Auditing and certification in the field of data security. In.: Gergely László Szőke (ed.): Privacy in the Workplace. Data Protection Law and Self-regulation in Germany and Hungary, HVG-ORAC, Budapest 2012, pp. 311-337.

[12] TONDEL, I. A., LINE, M. B., JAATUN, M. G., Information security incident management: Current practice as reported in the literature, Computers & Security, Volume 45, September 2014, Pages 42-57 doi:10.1016/j.cose.2014.05.003