JOURNAL OF MODERN SCIENCE

2/56/2024

www.jomswsge.com

DOI: doi.org/10.13166/jms/188911

MIROSŁAW KARPIUK

Warmia and Mazury University in Olsztyn, Poland

ORCID iD: orcid.org/0000-0001-7012-8999

SUPERVISION AND CONTROL OVER THE OPERATORS OF ESSENTIAL SERVICES, DIGITAL SERVICE PROVIDERS AND ENTITIES PROVIDING CYBERSECURITY SERVICES

Abstract

Threats in cyberspace are becoming increasingly burdensome to the users of information and communication systems. Therefore, their security constitutes a crucial part of activities conducted by operators of essential services, digital service providers, and entities providing cybersecurity services. Considering the necessity to ensure the proper protection of systems allowing activities in cyberspace, relevant entities must take actions related to supervision and control to assure compliance with the safety standards that reduce the threat of cybersecurity incidents.

The main objective of this paper is to analyse the legal regulations governing the issue of supervision and control of compliance with cybersecurity standards by entities responsible for safeguarding cyberspace against threats. Moreover, the paper also aims to characterise the supervision and control mechanisms designed to ensure the safe use of information and communication systems and to discuss the powers of supervision and control authorities.

The primary research method used in this paper is the doctrinal legal research method. It was applied to analyse the applicable legal regulations governing the supervision and control of activities in the sphere of securing cyberspace against attacks. In turn, the law theory method, also used in the studies whose results have been presented in this paper, allowed the assessment of actions being taken as part of supervision and control.

The fact that the issues of supervision and control in cybersecurity are subject to statutory regulations should be regarded as positive. However, these legal acts exhibit certain flaws. Some provisions regulating these issues are vague, which may result in their over-interpretation, and thus contribute to, among other things, the infringement of the freedom of business activities principle for enterprises operating in the cybersecurity sector.

Keywords: *cybersecurity, cyberspace, supervision, control, information and communication (ICT) system*

Introduction

Under Article 2 (4) of the National Cybersecurity System Act of 5 July 2018 (Journal of Laws 2023.913, consolidated text), *the NCSA*, cybersecurity is defined as the resilience of information systems against actions which compromise the confidentiality, integrity, availability and authenticity of processed data, or the related services provided by those information systems. Given the above, it refers to information systems, understood as information and communication systems with electronic data stored therein. As per Article 3 (3) of the Act of 17 February 2005 on the Computerisation of the Operations of Entities Carrying out Public Service Tasks (Journal of Laws 2023.57, consolidated text), an information and communication system is a set of cooperating IT hardware and software, providing a possibility to process and store, as well as send and receive, data via ICT networks with the use of an end device suitable for a given network type. These systems are likely to be targeted by cyber-attacks, so it is necessary to develop appropriate protection mechanisms which should keep pace with the dynamics of the threats that occur in cyberspace. In order to inspect whether such protection is handled in line with the assumptions made by the legislator, and to make potential interventions, legal instruments of supervision and control have been introduced.

Cybersecurity constitutes a specialised security system component which covers securing information systems against threats (Czuryk, 2019: 42), and security is a value that affects human behaviour in virtually every aspect of life (Ciesielski, 2019: 112). Cybersecurity involves counteracting and predicting threats and removing the outcomes resulting in relation to their occurrence. The sphere where such threats and their effects can be encountered is cyberspace (Karpiuk, 2021: 612). In the era of the digital state, where a vast majority of public activities are conducted using cyberspace, the significance of this security component is growing. Cybersecurity constitutes a vital part of security systems, both at the national and international levels.

The assurance of cybersecurity is one of the essential tasks that public authorities have been entrusted with. The consequences of IT-related threats are becoming increasingly severe. Cyber-attacks may be used to exert both economic and political pressure (Kaczmarek, 2019: 145).

Cyberspace does not exist entirely outside the realm of the physical world. Indeed, certain symptoms of cyberthreats and cyberattacks may transpire into the non-virtual space. Similarly, cyberspace can reveal signals of real-world threats (Włodyka, Kaczmarek, 2024: 264). Supervisory and inspection measures should account for these interrelations, particularly in the process of drawing conclusions to improve how providers of essential services, digital service providers and providers of cybersecurity services operate.

Supervision and control are frequent in public administration, which also refers to security and public order administration. Supervision can be described as shaping mutual relationships between specified entities where, in addition to control powers, the supervisory entity is also authorised to directly interfere in the operations of the entity under supervision (Polinceusz, 2013: 312). In turn, control is limited to observing and evaluating the conduct of the entity under control (Kostrubiec, 2013: 330; Nowikowska, 2018:41). As for supervision and control, in the sphere of meeting legal requirements related to cybersecurity on the part of operators of essential services, digital service providers, and providers of cybersecurity services, control authorities are also supervisory authorities.

Special protection must be extended to ICT systems involved in the implementation of specific tasks (of public significance) to guard them against cyberattacks and make sure these tasks can be carried on (Bencsik et al., 2024: 158). This special protection should be assessed as part of inspection measures.

The issues of cybersecurity are discussed by, *i.a.*, Andras Bencsik, Katarzyna Chałubińska-Jentkiewicz, Jarosław Kostrubiec, Krzysztof Kaczmarek, and Monika Nowikowska, and the issues of supervision and control in the sphere of cybersecurity are analysed by, for instance, Małgorzata Czuryk. While the subject matter of this paper is not new, it requires a more detailed analysis, in particular in the sphere of the normative solutions that have been adopted and their effectiveness.

Supervision and control authorities

Under Article 53 (1) of the NCSA, the legislator defined an exhaustive list of authorities in charge of supervising compliance with the provisions of the NCSA including the minister competent for computerisation and the competent authorities for cybersecurity. Supervisory authorities are, at the same time, control authorities.

The minister competent for computerisation manages the computerisation department which, as per Article 12a (1)(10) of the Act of 4 September 1997 on Government Administration Departments (Journal of Laws 2022.2512, consolidated text), covers the matters of cyberspace security in the civilian dimension. Therefore, such minister will not be competent to manage the military aspects of cybersecurity, as these belong to the powers of the Minister of National Defence.

Competent authorities for cybersecurity include relevant ministers, except the banking and financial market infrastructure sector, where such function is entrusted to the Polish Financial Supervision Authority, responsible for, *i.a.*, taking actions aimed at counteracting threats to the security of information and communication systems, as laid down in Article 4 (1)(3b) of the Financial Market Supervision Act of 21 July 2006 (Journal of Laws 2023.753, consolidated text). Given the above, supervision and control authorities are high in the public administration hierarchy. This demonstrates the great significance of cybersecurity protection issues. These authorities form the national cybersecurity system.

Entities subject to supervision and control

Entities subject to supervision and control include operators of essential services, digital service providers, and entities providing cybersecurity services (Nowikowska, 2022b: 347).

As per Article 5 (1) of the NCSA, an operator of essential services is an entity listed in the Annex to the NCSA, having an establishment on the territory of the Republic of Poland, in respect of which an authority competent for cybersecurity has issued a decision on recognising it as an operator of essential services. As a result of being granted the status of an operator of essential services, certain specified obligations are imposed on the entity. These include

those related to protecting the information systems being used for providing such services (Karpiuk, 2022: 166).

Not every entity can be identified as an operator of essential services, as it can only be an entity listed by the legislator in the Annex to the NCSA, defining strategic sectors and subsectors and the entities operating within them. It includes entities providing an essential service as defined in Article 2 (16) of the NCSA as a service necessary for maintaining critical societal and/or economic activities entered in the list of essential services. As essential services are of key importance for the societal and economic sphere, any disruptions to their provision may have an adverse effect on the functioning of the state and the society, resulting in various crises (Bencsik, Karpiuk, Kelemen, Włodyka, 2023: 15). For an entity to be identified as an operator of essential services, a competent authority for cybersecurity must issue a decision on recognising it as such an operator (Nowikowska, 2022a: 88).

Digital service providers are the second group of entities to be supervised and controlled in respect of compliance with the provisions of the NCSA governing cybersecurity rules. Pursuant to Article 17 (1) of the NCSA, a digital service provider is a legal person or an organisational unit without a legal personality and has its registered office or governing body based in Poland or a representative having an establishment in the territory of Poland, providing digital services, whereas micro – and small enterprises may not be digital service providers. A digital service is an electronically supplied service, which means that it is provided without the parties being simultaneously present (at a distance), through data transmission at the individual request of a recipient of such service, sent and received using electronic equipment for the processing (including digital compression) and storage of data, and entirely conveyed, received or transmitted via a telecommunications network, as stipulated in Article 2 (4) of the Act of 18 July on the Provision of Services by Electronic Means (Journal of Laws 2020.344, consolidated text). Digital services are also listed in the Annex to the NCSA.

Another group of entities that are identified in the context of control and supervision include entities providing cybersecurity services. The legislator has used a general and broad umbrella term here, taking into account all entities that provide services related to cybersecurity. Therefore, the list of entities

subject to supervision and control is very long. This results from the fact that cybersecurity is of great importance to the private and public sectors alike.

Notably, even the most technologically advanced cybersecurity tools will work only so far as users apply them. In some cases, institutions put in place cybersecurity procedures only after sustaining serious damage from a cyberattack. It should be remembered, however, that ensuring cybersecurity is not a one-time affair with a clear beginning and ending. Since systems are as resilient as their weakest links, it is necessary for institutions to consider every element of their respective systems, even those seemingly negligible, that can impact their overall functioning (Kaczmarek, 2024: 112). Providers of essential services, digital service providers and providers of cybersecurity services must bear this in mind as well, otherwise they may face consequences of supervisory reviews or inspections, should these identify any shortcomings.

The scope of and procedure for supervision and control

In addition to the continuity of tasks being performed by relevant authorities, the security sphere also requires their actions to be effective, not only in respect of an ongoing response to threats, but also in relation to anticipating and preventing them, as well as undertaking remedial measures. Such effectiveness might be reached if proper control and supervision measures are adopted in the security sphere (Karpiuk, 2024:11). This also applies to cybersecurity.

Under Article 53 (1)(1) of the NCSA, the minister competent for computerisation exercises supervision in the sphere of ensuring compliance with cybersecurity requirements by entities providing cybersecurity services, which includes: 1) meeting organisational and technical conditions which allow the assurance of cybersecurity to operators of essential services; 2) having premises intended for the provision of incident response services secured against physical and environmental threats; 3) applying safeguards to ensure the confidentiality, integrity, availability and authenticity of the processed information, taking into account personal safety and system operation and architecture. The conformity with these basic requirements is subject to supervision and control.

Entities providing cybersecurity services are obliged to meet the following conditions: 1) the obligation to have, maintain, and update an information safety management system that is consistent with specified requirements, 2) to ensure the continuity of an incident handling service and the support to operators of essential services with a response time adequate for the nature of a given essential service; 3) to have and provide access to its operation policy declaration in Polish and English; 4) have personnel with specified skills; 5) have the exclusive right to use premises or a complex of premises; 6) conduct a risk analysis aimed at selecting adequate measures for the physical and technical security of premises or a complex of premises where cybersecurity services are provided, in which all the significant factors that may affect security are taken into account. The obligations are stipulated in § 1 (1) of the Regulation of the Minister of Digital Affairs of 4 December 2019 on the technical and organisational conditions for entities providing cybersecurity services and internal organisational structures of operators of essential services in charge of cybersecurity (Journal of Laws, 2019.2479). Meeting these conditions is the subject matter of activities arising from supervision and control regarding entities providing cybersecurity services.

The scope of supervision on the part of competent authorities for cybersecurity is specified in Article 53 (1)(2) of the NCSA and includes: 1) performing obligations related to counteracting cybersecurity threats and notifying about serious incidents by the operators of essential services; 2) meeting security requirements in respect of digital services rendered by digital service providers and performing obligations related to notifying about substantial incidents. Given the above, supervision covers both meeting cybersecurity standards and performing the obligation to notify about incidents (Nowikowska, 2021b: 85).

As part of the supervision in the sphere of compliance with cybersecurity laws, under Article 53 (2) of the NCSA, a competent authority for cybersecurity or a minister competent for computerisation conducts inspections in the said respect, and the competent authority for cybersecurity imposes financial penalties on the operators of essential services and digital service providers. The minister competent for computerisation is also an authority competent for cybersecurity (for the digital infrastructure sector). Hence the provision may be misleading because the minister may also charge financial

penalties, yet not on entities providing cybersecurity services, but on the operators of essential services and digital service providers.

In the first stage of examining compliance with the NCSA, the relevant authority conducts an inspection covering the performance of obligations that concern counteracting threats to cybersecurity and notifying about incidents, and meeting the requirements that allow the assurance of cybersecurity, including the security of the digital services being provided, and then, if any irregularities are found, the competent authority for cybersecurity may impose a financial penalty on the entity being subject to supervision (Czuryk, 2022b: 114-115).

As stipulated in Article 47 (1) of the Enterprise Law of 6 March 2018 (Journal of Laws 2023.221, consolidated text), control activities are planned and conducted after a prior analysis of the probability that legal regulations may be violated in the course of given business activities. The analysis includes identifying subjective and objective areas where the risk of law infringement is the highest. This refers to both operators of essential services and digital service providers being enterprises and entities providing cybersecurity services (notwithstanding their status), but does not apply to the operators of essential services and digital service providers that are not enterprises.

As per Article 59 of the NCSA, if, based on the information included in the inspection report, a competent authority for cybersecurity or the minister competent for computerisation finds that the provisions of the NCSA could be violated by the entity subject to control, follow-up recommendations are given to remove the irregularities. There are no appeals measures available in respect of the recommendations. The entity subject to control is obliged to inform the control authority of the method of carrying out the follow-up recommendations within the specified time limit. The enterprise concerned does not have any possibility to request another authority to verify the correctness of follow-up recommendations but is obliged to perform them. As stipulated in Article 73 (1)(13) of the NCSA, an operator of an essential service that has failed to implement follow-up recommendations within a set time limit is subject to a financial penalty.

If, as a result of control, the competent authority for cybersecurity finds that a given operator of essential services or a digital service provider is in persistent breach of the provisions of the NCSA, causing: 1) direct and serious

cybersecurity threat to state defence and security, public safety and order or the life and health of people, 2) risk of serious property loss or serious disruptions in the provision of essential services, the authority may impose a fine of up to PLN 1,000,000 under Article 73 (5) of the NCSA.

Regarding the operators of essential services and digital service providers that are not enterprises, the applicable law is the Act of 15 July 2011 on Control in Government Administration (Journal of Laws 2020.224, consolidated text) (Nowikowska, 2021a: 10).

Under Articles 3–4 of the Act, the purpose of an inspection is to assess how the inspected entity operates based on established facts and a defined set of criteria. If any irregularities are found, an inspection should also determine their scope, causes and effects, as well as identify those accountable for them and issue recommendations for remediation. Inspections are concerned with aspects such as legality, economic efficiency, viability and diligence, unless there is specific legislation to the contrary. In accordance with Article 14 of the Act, before an inspection is conducted, an inspection programme must be drafted and approved by the Inspection Unit's manager. The following should be particularly taken into account when drafting the programme: 1) previous inspection findings; 2) results of investigations and analyses, and any complaints and requests related to the prepared inspection; 3) any risk factors affecting the operations of the entity to be inspected; and 4) any information on the operations of the entity to be inspected.

It should be stressed that threat analysis, in particular the response to incidents, including their detection, examination of interference areas, their elimination, restoring the original conditions, and mitigation of the possibility of similar interference in the future, is the essence of rational combat against cyber-threats (Pizło, 2022: 139). It needs to be considered in the course of supervision or control activities, given that such evaluation covers measures to counteract cybersecurity threats and the notification of (serious and substantial) incidents.

Conclusions

The entities of the national cybersecurity system (including operators of essential services, digital service providers or entities providing cybersecurity services) must engage in the fulfilment of objectives set for the system, which include the assurance of cybersecurity at the national level (general objective), entailing the following specific objectives: 1) uninterrupted provision of essential services and digital services; 2) assurance of a proper level of security of information systems being used for the provision of these services, 3) assurance of incident handling (Karpiuk, 2023: 192). They are their statutory obligations, so the fulfilment of the objectives is reviewed as part of control activities.

The development of capabilities and methods allowing interference with information and communication systems is expansive. The expansive nature is directly proportional to the number of such systems and participants and the volume of the capital flowing through the systems (Konaszczuk, 2021: 338). The mechanisms that protect cyberspace against threats must keep pace with the development. But to this end, operators of essential services, digital service providers, and entities providing cybersecurity services must meet proper organisational and technical conditions. Failure to observe these conditions may lead to specific consequences, including burdensome financial penalties imposed by the control authority.

Information and communication systems are not intended only for searching for information but also for conducting business activities, rendering various types of services, communicating, and performing public tasks, and as they are of strategic significance for the state and the economy, they need to be duly protected (Czuryk, 2022a: 40). Control and supervision are to ensure such protection.

It should be emphasised that cyberspace threats to the functioning of society and the state do not arise solely from the existence of ICT infrastructure but from the possibilities such infrastructure can produce (Kaczmarek, 2022: 34). To ensure the safe use of the infrastructure, relevant entities (including service providers) must duly focus on the security of the services they offer, to minimise the occurrence of incidents, whereas the analysis of such safeguards is conducted as part of supervision and control measures.

Control is aimed at evaluating the operations of the entity subject to control in terms of compliance with cybersecurity laws based on the facts established by the control authority. If any material weaknesses are found that may affect security in cyberspace, the relevant authority may take any necessary intervention measures as part of its supervision powers.

The legal regulations concerning security architecture must, on the one hand, take into account the freedom of service provision in cyberspace and, on the other hand, keep a lookout for continuous threats concerning unlawful interference with information and communication systems which are intended to provide such services and at the same time allow their use by customers. The security of such systems is becoming crucial to their normal functioning, in which disruptions are unable to affect the activities that are performed in cyberspace. The protection of cyberspace should be an essential part of public policies, which are implemented by way of supervision and control.

Although the public relies heavily on digital services, there is often a lack of awareness of how to use them safely. This not only calls for educational measures, but also requires that providers of digital services introduce suitable and adequate safeguards to protect against cyberthreats (Czuryk, 2024: 45). The application of these measures should be subject to supervision and inspection.

Entities responsible for the functioning of ICT systems have the obligation to ensure cybersecurity for these systems (Evsyukova et al., 2024: 59). Failure to meet this requirement may warrant supervisory measures against them.

It is important to note that risks associated with cyberattacks are often concealed, most likely for the sake of financial benefit (Kaczmarek, 2024: 159). The role of supervisory and inspection measures is to prevent this.

What is more, some legislation concerning supervision over, and inspection of, providers of essential services, digital service providers and providers of cybersecurity services is not as clear as it should be, given that the economic sphere is involved. This may lead to undermining the economic freedom of cybersecurity businesses.

Pursuant to Article 5(2) of the NCSA, the competent authority for cybersecurity issues a decision to recognise an entity as an operator of an essential service if: 1) such an entity provides an essential service; 2) the provision of the service relies on information systems; 3) a security incident could disrupt

the rendering of an essential service by that provider. These prerequisites allow regulatory interference with economic freedom, and by recognising an entity as an operator of an essential services, it is possible to supervise and inspect it.

Pursuant to Article 14(2) of the NCSA, the internal cybersecurity structures established by operators of essential services and providers of cybersecurity services are required to: 1) fulfil the organisational and technical conditions to ensure cybersecurity for operators of essential services; 2) have at their disposal facilities designed to provide incident-response services that are secured against physical and environmental threats; 3) have in place protections that ensure confidentiality, integrity, accessibility and authenticity of the processed information while recognising personal safety and the system's operation and architecture. The fulfilment of these requirements is subject to supervision and inspection, with the supervisory authority having a certain margin of freedom that may undermine economic freedom.

References

Bencsik, A., Karpiuk, M., Kelemen, M., Włodyka, E. (2023). *Cybersecurity in the Visegrad Group Countries*. Maribor: Lex Localis Press.

Bencsik, A., Karpiuk, M., Strizzolo, N. (2024). *Cybersecurity of E-government*, 12(2), 146-160. Cybersecurity and Law.

Ciesielski, M. (2019). *Socjologia bezpieczeństwa jako subdyscyplina nauk o bezpieczeństwie* 2(2), 109-134. Cybersecurity and Law.

Czuryk, M. (2019). *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, 2(2), 39-50. Cybersecurity and Law.

Czuryk, M. (2022a). *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, 31(3), 31-43. Studia Iuridica Lublinensia.

Czuryk, M. (2022b). Supervision and Inspection in the Field of Cybersecurity, in M. Karpiuk, J. Kostrubiec (Eds.), *The Public Dimension of Cybersecurity*, 111-119. Maribor: Lex Localis Press.

Czuryk, M. (2024). *The Legal Status of Digital Service Providers in the National Cybersecurity System*, 11(1), 39-46. Cybersecurity and Law.

Evsyukova, O., Karpiuk, M., Kelemen M. (2024). *Cyberthreats in Ukraine, Poland and Slovakia*, 11(1), 58-78. Cybersecurity and Law.

Kaczmarek, K. (2019). *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii,* 1(1), 143-157. Cybersecurity and Law.

Kaczmarek, K. (2022). Digital Competencies of the General Public and the State's Vulnerability to Cyberspace Threats, in M. Karpiuk, J. Kostrubiec (Eds.), *The Public Dimension of Cybersecurity*, 29-37. Maribor: Lex Localis Press.

Kaczmarek, K. (2024). *Nordic Countries in the Face of Digital Threats*, 11(1), 151-161. Cybersecurity and Law.

Kaczmarek, K. (2024). *Vulnerability to Cyber Threats: A Qualitative Analysis From Societal And Institutional Perspectives*, 12(2), 106-116. Cybersecurity and Law.

Karpiuk, M. (2021). *The Local Government's Position in the Polish Cybersecurity System*, 19(3), 609-620. Lex Localis – Journal of Local Self-Government.

Karpiuk, M. (2022). *Recognizing an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level*, 42(4), 166-179. Prawo i Więź.

Karpiuk, M. (2023). *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, 32(2), 189-201. Studia Iuridica Lublinensia.

Karpiuk, M. (2024). *Audyt, kontrola i nadzór w sferze bezpieczeństwa*. Warsaw: ASzWoj.

Konaszczuk, W. (2021), *Cybersecurity Threats in the Sectors of Oil, Natural Gas and Electric Power in the Context of Technological Evolution*, 30(4), 333-351. Studia Iuridica Lublinensia.

Kostrubiec, J. (2013). Kontrola administracji publicznej, in: M. Karpiuk, J. Kowalski (Eds.), *Administracja publiczna i prawo administracyjne w zarysie*, 329-364. Warszawa-Poznań: Iuris.

Nowikowska, M. (2018). *Ocena funkcjonalności systemu kontroli w Siłach Zbrojnych RP*. Warsaw: Towarzystwo Wiedzy Obronnej

Nowikowska, M. (2021a). Cele i funkcje kontroli, in: M. Nowikowska, K. Chałubińska-Jentkiewicz (Eds.), *Ustawa o kontroli w administracji rządowej. Komentarz*, 10-19. Warsaw: C.H. Beck.

Nowikowska, M. (2021b). *Nadzór i kontrola operatorów usług kluczowych, dostawców usług cyfrowych i podmiotów świadczących usługi w zakresie cyberbezpieczeństwa*, 5(1), 77-103. Cybersecurity and Law.

Nowikowska, M. (2022a). Protection of Critical Infrastructure in Cyberspace, in M. Karpiuk, J. Kostrubiec (Eds.), *The Public Dimension of Cybersecurity*, 79-92. Maribor: Lex Localis Press.

Nowikowska, M. (2022b). The System of Control and Supervision of Operators of Essential Services, Digital Service Providers and Entities Providing Cybersecurity Services, in K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński (Eds.), *Cybersecurity in Poland, Legal Aspects*, 347-364. Cham: Springer.

Pizło, W. (2022). Management in Cyberspace: From Firewall to Zero Trust, in M. Karpiuk, J. Kostrubiec (Eds.), *The Public Dimension of Cybersecurity*, 133-146. Maribor: Lex Localis Press.

Polinceusz, M. (2013). Nadzór nad administracją publiczną, in: M. Karpiuk, J. Kowalski (Eds.), *Administracja publiczna i prawo administracyjne w zarysie*, 311-327. Warszawa-Poznań: Iuris.

Włodyka, E.M., Kaczmarek, K. (2024). *Cyber Security of Electrical Grids – A Contribution to Research*, 12(2), 260-272. Cybersecurity and Law.