Cybersecurity in the European Union Law

Filip Radoniewicz

Abstract The first legal acts adopted within the framework of the European Communities were adopted in the early nineties. However, they were not binding. They contained calls for appropriate actions, identification of some solutions, proposals for draft legal acts, strategies and action plans to improve network security.

This chapter, however, highlights the most important binding acts: the first binding EU legal instrument to combat computer crime: Council Framework Decision 2005/222/JHA of the 24th of February 2005 on attacks against information systems, Directive 2013/40/EU of the European Parliament and of the Council of the 12th of August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA and Directive (EU) 2016/1148 of the European Parliament and of the Council of the 6th of July 2016 concerning measures for a high common level of security of network and information systems across the Union.

1 Introduction

When discussing European Union activities in the field of cybersecurity and combating cybercrime, it appears advisable to go back to the 1990s, when the first non-binding legal Acts were adopted to regulate these matters. They called for the implementing of the appropriate measures, indicating specific solutions or proposals for the draft legal Acts, as well as the developing of strategies and action plans to improve network security. In this context, the following documents are worth noting:

F. Radoniewicz (✉)
Akademickie Centrum Polityki Cyberbezpieczeństwa/Academic Center for Cybersecurity Policy, Akademia Sztuki Wojennej w Warszawie/War Studies University in Warsaw, Warsaw, Poland
e-mail: filip.radoniewicz@radoniewicz.eu

K. Chałubińska-Jentkiewicz et al. (eds.), *Cybersecurity in Poland*,
https://doi.org/10.1007/978-3-030-78551-2_6

1. Council Decision 92/242/EEC of the 31st of March 1992 in the Field of Security of Information Systems;[1]
2. Council Recommendation 95/144/EC of the 7th of April 1995 on Common Information Technology Security Evaluation Criteria;[2]
3. Communication COM(2000)890 EU from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions of the 26th of January 2001: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime (the so-called Communication on Cybercrime);
4. The Resolution of Parliament of the 19th of May 2002 Calling for Legislative Measures Against High-Tech Crime;[3]
5. Communication COM(2001)298 from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, of the 6th of June 2001: Network and information security: Proposal for a European policy approach;[4]
6. Council Recommendation of the 25th of June 2001 on Contact Points Maintaining a 24-h Service for Combating High-Tech Crime;[5]
7. The Council Resolution of the 28th of January 2002 on a Common Approach and Specific Actions in the Field of Network and Information Security;[6]
8. Communication COM (2006)251 from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, of the 31st of May 2006: A strategy for a secure information society: Dialogue, partnership and empowerment;
9. Communication COM (2006)288 from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, of the 15th of July 2006 on counteracting spam, spyware and malicious software;
10. Communication COM (2007)267 from the Commission to the European Parliament, the Council and the Committee of the Regions of the 22nd of May 2007: Towards a general policy on the cybercrime prevention, extending the so-called Communication on Cybercrime of 2001;

[1]Council Decision 92/242/EEC of 31 March 1992 in the Field of Security of Information Systems (OJ EU L 123/19).

[2]Council Recommendation 95/144/EC of 7 April 1995 on Common Information Technology Security Evaluation Criteria, OJ EC 1995 C 93/27.

[3]The Resolution of Parliament of 19 May 2002 Calling for Legislative Measures Against High-Tech Crime, Unpublished.

[4]Unauthorised access to information systems, disruptive attacks on information systems, malicious software, misrepresentation (using other person's data with fraudulent intentions—this not only concerned identity theft but also spoofing).

[5]Council Recommendation of 25 June 2001 on Contact Points Maintaining a 24-h Service for Combating High-Tech Crime Official Journal C 187 of 3.07.2001, p. 5.

[6]The Council Resolution of 28 January 2002 on a Common Approach and Specific Actions in the Field of Network and Information Security, OJ EC 2002 C 43/2.

11. Communication COM (2009)149 from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions of the 30th of March 2009 on Critical Information Infrastructure Protection: Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience" together with a report on multi-annual wide-scale European consultations regarding network security;[7]
12. Commission Staff Working Document—Assessment of the EU 2013 Cybersecurity Strategy;[8]
13. Council Decision of the 23rd of September 2013 on the Security Rules for Protecting EU Classified Information (2013/488/EU);[9]
14. Joint Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.[10]
15. The *eEurope – An Information Society for All* initiative was launched at the end of 1999.[11] The Communication regarding the Commission's initiative was prepared for the special meeting of the European Council in Lisbon on the 23rd–24th of March 2000, the objective of which was to streamline the activities facilitating the creation of an information society. It was stressed in the Communication that the computerisation process must cover all aspects of European residents' lives, including in particular work, home, school, university, healthcare, transport, and contacts with public administration. The document identified ten fields on which special emphasis should be placed with a view to building an information society. According to Kuliński, these fields can be divided into three groups, centred on infrastructure (ensuring low-cost access to the Internet, and building fast Internet connections intended for scientific and academic circles),
16. research and education (in particular, providing Internet connections in schools, and supporting small and medium-sized enterprises in implementing advanced technologies),
17. applications (accelerating the development of e-commerce, smart cards, e-health, e-government, smart transport).[12]

At the aforementioned special meeting of the European Council, which took place in Lisbon on the 23rd–24th of March 2000, the eEurope programme was

[7]Radoniewicz (2016), pp. 233–236.

[8]Commission Staff Working Document—Assessment of the EU 2013 Cybersecurity Strategy SWD (2017) 295 final of 13.9.2017.

[9]Council Decision of 23 September 2013 on the Security Rules for Protecting EU Classified Information (2013/488/EU), OJ EU 2012 L 27/1.

[10]Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN(2013) 1 final.

[11]Commission Communication COM (1999) 687: *eEurope – An Information Society for All*.

[12]Kuliński (2010), pp. 23–24. Cf. Chałubińska-Jentkiewicz (2019), pp. 266–269.

approved, and the so-called Lisbon Strategy was adopted. The Lisbon Strategy was a long-term socio-economic development programme for the European Union, the purpose of which was to make Europe the most dynamic and competitive economic region in the world by building the knowledge-based economy (i.e. an economy directly based on production, distribution, and the use of information and knowledge).[13]

In June 2000, at the meeting in Santa Maria de Feira, *eEurope 2002 – An Information Society for All. Action Plan* was adopted.

The measures implemented within the framework of the eEurope 2002 programme were maintained in the eEurope 2005 programme, and then in the i2010 Strategy announced in Commission Communication COM(2005)229 of the 1st of June 2005: *i2010 – A European Information Society for Growth and Employment. Europe 2020 – A strategy for smart, sustainable and inclusive growth* (COM (2010)2020), which was approved by the European Council on the 17th of June 2010, serves as a follow-up to the i2010 programme. It is within its framework that the European digital agenda has been implemented. Its objective is to develop a uniform digital market enabling EU Member States to derive permanent economic and social benefits.

At the meeting of the European Council which took place on the 4th–5th of November 2004 in Brussels, an action plan in the fields of justice and internal affairs was adopted. It was referred to as the Hague Programme, as it was developed during the Netherlands' Presidency of the Council of the European Union.

The Hague Programme's implementation was continued in the so-called Stockholm Programme—*An Open and Safe Europe Serving and Protecting Citizens*—adopted during Sweden's Presidency at the meeting in Brussels on the 10th–11th of December 2009. It was implemented within the framework of the action plan adopted by the Commission on the 20th of April 2010. It recommended that an internal security strategy be developed for the EU, directed at increasing the protection of citizens and at effectively combating serious crime, organised crime, and terrorism, by strengthening cooperation between the police and the judicial services in criminal cases, and Member States' cooperation in the field of border management, citizen protection and assistance in the event of natural disasters or catastrophes. Other guidelines regarding the development planning of the AFSJ (the area of freedom, security and justice) were laid down by the European Council on 26th–27th of June 2014. However, these were not turned into a programme, as had been done with previous guidelines, but were included in the European Union conclusions. In the document entitled *The Continuation of Work on a Comprehensive Approach to Cybersecurity and Cybercrime,* ensuring cybersecurity was considered a principal measure directed at providing EU citizens with real security space.[14]

[13]See more e.g. Radoniewicz (2019a), pp. 13–14.

[14]Chałubińska-Jentkiewicz (2019), pp. 269–270.

On the 6th of May 2015, *A Digital Single Market Strategy*[15] was adopted, its purpose being to develop a uniform legal framework for the EU digital market.

2 Council Framework Decision 2005/222/JHA of the 24th of February 2005 on Attacks Against Information Systems

Council Framework Decision 2005/222/JHA of the 24th of February 2005 on attacks against information systems[16] was the first binding EU legal instrument the objective of which was to combat computer crime. In principle, the document included definitions of the most pertinent concepts ("information system," "computer data," "legal person" and "without right"), and obliged Member States to consider illegal access to information systems and illegal system interference as punishable offences. Reference was also made to the liability of legal persons, jurisdiction, and the establishing of a network of points of contact' maintaining a 24-h service, available 7 days a week, to facilitate the exchange of information on attacks against information systems. The limited number of crimes defined in Framework Decision 2005/222, along with the need to recognise new threats, as well as the intent to adjust the regulations to new EU initiatives in the field of cybersecurity, and to supplement them in order to arrive at a comprehensive regulation of this subject matter, eventually led to a decision on developing a new legal instrument concerning cybercrime. Work on the new regulation coincided with the adopting of the Treaty of Lisbon, which made it possible to use the directive for regulating cybercrime issues.

3 Directive 2013/40/EU of the European Parliament and of the Council of the 12th of August 2013 on Attacks Against Information Systems

In Directive 2013/40/EU of the European Parliament and of the Council of the 12th of August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA,[17] the provisions of Framework Decision

[15] *A Digital Single Market Strategy* Communication COM (2015)192 from the Commission to the European Parliament, the Council, the Economic and Social Committee, and the Committee of the Regions. Cf. Radoniewicz (2019a), pp. 14–15.

[16] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OJ EU 2005 L 69/67.

[17] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ EU 2013 L218/8.

2005/222 were generally upheld, but a number of new solutions were added. New types of criminal offences were envisaged (e.g. the illegal interception of computer data, and crimes involving "hacking tools"), and additional circumstances were defined, along with committing crime within a criminal organisation, as provided for in Framework Decision 2005/222 (though with more stringent sanctions), which Member States should obligatorily treat as increasing criminal liability. These included 'botnet' attacks, causing serious harm (such issues as causing serious harm or influencing material interests were also envisaged in the Framework Decision, but that provision was of a non-obligatory character), committing an offence against an information system with critical-infrastructure status, and another person's true identity's being used by the perpetrator.[18]

4 Directive 2017/541 (EU) of the European Parliament and of the Council of the 15th of March 2017 on Combating Terrorism

Directive 2017/541/EU of the European Parliament and of the Council, of the 15th of March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA[19] and amending Council Decision 2005/671/JHA,[20] is the major legal instrument whose purpose is to combat terrorism in the European Union. Under Article 3 of Directive 2017/541, in order for an illegal act to be considered a terrorist offence, it must meet the objective criterion of being one of the acts listed in the closed-ended list contained in that article, or involve a threat of such an act's being committed. In addition, it must satisfy at least one of the premises listed further in the definition, concerning the perpetrator's purpose, i.e. it must be committed with the intention of

1. seriously intimidating a population, or
2. unduly compelling a government or an international organisation to perform or abstain from performing any act, or
3. seriously destabilising or destroying the fundamental political, constitutional, economic, or social structures of a country or an international organisation.

The list referred to above contains, *inter alia*, the illegal acts as defined in Articles 4 and 5 of Directive 2013/40 (illegal system interference and illegal data interference, respectively) provided that any of the aggravating circumstances listed in the directive are found to have occurred (as regards the act defined in Article 4, when the

[18] See more e.g. Radoniewicz (2017), pp. 303–317.

[19] About Framework Decision 2002/475/JHA see e.g. Radoniewicz (2015), pp. 192–196.

[20] Directive 2017/541/EU of the European Parliament and of the Council, of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ EU 2017 L 88/6.

perpetrator's action involving the use of hacking software affected a large number of information systems, or the act caused serious damage to or was directed against an information system with critical-infrastructure status; and as regards the act as defined in Article 5, when the act was committed against an information system with critical-infrastructure status).[21] Furthermore, Member States were obliged to take the necessary measures to ensure the prompt removal of online content constituting a public provocation to commit a terrorist offence, or to block access to such content when its removal is not feasible (Article 21 of Directive 2017/541).[22]

5 Directive 2008/114/EC of the 8th of December 2008 on the Identification and Designation of European Critical Infrastructures

With a view to raising the security level of critical infrastructures of supra-national significance, Council Directive 2008/114/EC of the 8th of December 2008 on the identification and designation of European critical infrastructures, and the assessment of the need to improve their protection, was adopted.[23] Under Article 2(a) of the Directive, "critical infrastructure" means an asset, system, or part thereof located in Member States, which is essential for the maintenance of vital societal functions: health, safety, security, the economic or social well-being of people, the disruption or destruction of which would have a significant impact on a Member State as a result of the failure to maintain those functions; and "The European critical infrastructure", or "ECI", as defined in Article 2(b) of the Directive, means a critical infrastructure located in Member States whose disruption or destruction would have a significant impact on at least two Member States. The significance of this impact is assessed in terms of cross-cutting criteria. These include the effects resulting from cross-sector dependencies on other types of infrastructure. Under Article 3(2) of the Directive, the cross-cutting criteria comprise the casualties' criterion, the economic-effects' criterion, and the public-effects' criterion. While the Directive is focused on the energy and transport sectors, its extension is planned to include other sectors, e.g. the information-and-communication-technology (ICT) sector.

[21] See more: Radoniewicz (2016), pp. 266–267.

[22] See more e.g. Radoniewicz (2019b), pp. 193–205.

[23] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance), OJ EU 2008 L 345/7.

6 Directive 2002/21/EC on a Common Regulatory Framework for Electronic Communications Networks and Services (A Framework Directive)

Directive 2002/21/EC of the European Parliament and of the Council of the 7th of March 2002 on a common regulatory framework for electronic communications networks and services (A Framework Directive)[24] lays down a common regulatory framework for electronic-communications networks, i.e. transmission systems, which permit the conveyance of signals by wire, radio, optical, or other electromagnetic means, including satellite networks, fixed and mobile terrestrial networks, electricity-cable systems, networks used for radio and television broadcasting, and cable-television networks, irrespective of the type of information conveyed, as well as for electronic-communications services, which consist of the conveyance of signals on those networks, and the associated equipment and services related to electronic-communications networks and services, which facilitate or support the provision of services by such networks. It also lays down tasks of national regulatory authorities, and establishes a set of procedures to ensure the harmonised application of the regulatory framework throughout the Community (Article 1(1) of Directive 2002/21/EC).

The issue of network security is discussed in Chapter IIIa of Directive 2002/21/EC, which was added by way of a directive 2009/140/EC of the 25th of November 2009,[25] which became effective on the 19th of December 2009.

Under Article 13a (1) of Directive 2002/21/EC, Member States were obliged to ensure that undertakings providing public-communications networks or publicly available electronic-communications services take the appropriate technical and organisational measures to properly manage the risks posed to the security of networks and services. These measures are expected to ensure a level of security commensurate to the risk presented, having regard to the state of the art. In particular, measures should be taken to prevent and minimise the impact of security incidents on users and interconnected networks.

Member States are also required to ensure that undertakings providing public-communications networks take all the appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of the supply of the services provided over those networks (Article 13a (2) of Directive 2002/21/EC), and that undertakings providing public-communications networks or publicly available electronic-

[24]Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ EC 2002 L 108/33.

[25]Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (OJ EU 2013 L 337/37).

communications services take the appropriate technical and organisational measures to properly manage the risks posed to the security of networks and services (Article 13a (3) of Directive 2002/21/EC).

With a view to implementing the provisions of Article 13a, the responsible national regulatory authorities need to be vested with the power to issue binding instructions, including those regarding time limits for implementation, to undertakings providing public-communications networks or publicly available electronic-communications services (Article 13b (1) of Directive 2002/21/EC).

Under Article 13b (2) of Directive 2002/21/EC, undertakings providing public-communications networks or publicly available electronic-communications services should be required to notify the responsible national regulatory authority of every breach of security or loss of integrity, which has had a significant impact on the operation of networks or services.

Member States are expected to ensure that the responsible national regulatory authorities have the power to require undertakings providing public-communications networks or publicly available electronic-communications services to

(a) provide the information needed to assess the security and/or integrity of their services and networks, including documented security policies; and
(b) submit to a security audit performed by a qualified independent body or a responsible national authority, and make the results thereof available to the national regulatory authority. The cost of the audit will be met by the undertaking (Article 13b (2) of Directive 2002/21/EC).

Article 13b (3) of Directive 2002/21/EC provides for vesting national regulatory authorities with all the powers necessary to investigate cases of non-compliance and the effects thereof on the security and integrity of networks.

7 Directive 2006/24/EC on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks

Directive 2006/24/EC of the European Parliament and of the Council of the 15th of March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC,[26] aimed to

[26]Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ EU 2006 L 105/54 (no longer in force).

harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic-communications services or of public-communications networks in respect of the retention of so-called transmission data (i.e. traffic and location data, and related data necessary to identify the subscriber or registered user) which are generated or processed by them, in order to ensure that the data are available for the purposes of the investigation, detection, and prosecution of serious crimes, as defined by each Member State in its national law (Article 1). At the same time, the Directive (in Article 3) obliges Member States to adopt measures to ensure that these data (specified in detail in Article 5) are retained in accordance with the provisions thereof, to the extent that they are generated or processed by providers of publicly available electronic-communications services, or of a public-communications network within their jurisdiction, in the process of supplying the communications services concerned. The obligation to retain data includes the retention of data in the event of unsuccessful call attempts where those data are generated or processed and stored (as regards telephone data) or saved while users' logging in (as regards Internet data), by providers of publicly available electronic-communications services, or of a public-communications network within the jurisdiction of the Member State involved in the process of supplying the communications services concerned. Under Article 6, these categories of data are retained for periods of not less than six months and not more than two years from the date of the communication. This Directive was implemented by Member States (obviously including Poland) but it was then deemed invalid by the Court of Justice decision of the 8th of April 2014.[27] However, the decision did not cause all the provisions adopted in the course of the Directive transposition to be repealed. The basis for data retention in EU law is thus still provided by Article 15(1) of the Privacy Directive.

8 Regulation No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS)

Regulation (EU) No 910/2014 of the European Parliament and of the Council of the 23rd of July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC[28] (eIDAS) lays down a new system of secure electronic interactions across the EU between businesses, citizens, and public authorities.

[27]Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd vs. the Minister for Communications et al., ECLI:EU:C:2014:238.

[28]Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ EU 2014 L 257/73, (hereinafter referred as eIDAS).

1. It also lays down the conditions under which Member States recognise electronic-identification means of natural and legal persons falling under a notified electronic-identification scheme of another Member State,
2. It lays down the rules for trust services, in particular for electronic transactions, and
3. It establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered-delivery services, and certificate services for website authentication (Article 1).

Under the regulation on trust services, qualified and non-qualified trust-service providers[29] are obliged to take the appropriate technical and organisational measures, having regard to the latest technological developments, to manage the risks posed to the security of the trust services they provide, while also ensuring that the level of security is commensurate to the degree of risk. In particular, they are expected to take measures to prevent and minimise the impact of security incidents, and to inform stakeholders of the adverse effects of any such incidents.

Qualified and non-qualified trust-service providers must, without undue delay, but in any case within 24 h after having become aware of it, notify the supervisory body, and, where applicable, other relevant bodies, such as the authorised national body for information security or the data-protection authority, of any breach of security or loss of integrity which has a significant impact on the trust service provided, or on the personal data maintained therein. Furthermore, where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trust service has been provided, the trust-service provider must also notify the natural or legal person of the breach of security or loss of integrity without undue delay. Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body is obliged to inform the supervisory authorities in the other Member States concerned, and ENISA (The European Network and Information Security Agency; currently—The European Union Agency for Cybersecurity).

[29]Under Article 3(19), in conjunction with Article 3(20) of the Regulation on trust services, the term "trust-service provider" means a natural or a legal person who provides one or more trust services, either as a qualified (i.e. satisfying certain additional requirements stipulated in the regulation) or as a non-qualified trust-service provider. "Trust service" means an electronic service normally for remuneration which consists of:

(1) the creation, verification, and validation of electronic signatures, electronic seals, or electronic time stamps, electronic registered delivery services and the certificates related to those services; or
(2) the creation, verification, and validation of certificates for website authentication; or
(3) the preservation of electronic signatures, seals, or certificates related to those services.

Finally, "qualified trust service" means a trust service which meets the applicable requirements laid down in the regulation on trust services.

9 Directive 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union

The draft version of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)[30] was presented in 2013 as a major element in the Cybersecurity Strategy, its underlying objective being to ensure a high level of security of network and information systems (hence the Directive is commonly abbreviated as the NIS Directive) at the EU level, i.e. to increase the security of tele-information systems forming the basis for the functioning of the modern societies and economies of EU Member States, which is to improve the functioning of the EU internal market. To this end, Article 2(1) of the NIS Directive provides for

1. laying down obligations for all Member States to adopt a national strategy on the security of network and information systems
2. creating a cooperation group in order to support and facilitate strategic cooperation and the exchange of information among Member States, and to develop trust and confidence amongst them creating a computer security incident response team (CSIRT) network in order to contribute to the development of trust and confidence between Member States, and to promote swift and effective operational cooperation
3. establishing security and notification requirements for operators of essential services and for digital service providers
4. laying down obligations for Member States to designate the responsible national authorities, single points of contact, and CSIRTs, with tasks related to the security of network and information systems.

The requirements concerning security and incident reporting, as stipulated in the NIS Directive, are not applicable to undertakings which are subject to the requirements arising from Articles 13a and 13b of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002, on a common regulatory framework for electronic communications networks and services (A Framework Directive) (i.e. to undertakings providing public-communications networks or publicly available electronic-communications services), or to trust-service providers which are subject to the requirements arising from Article 19 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of the 23rd of July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[30]Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ EU 2016 L 194/1, (hereinafter referred as "NIS Directive").

The NIS Directive is without prejudice to the actions taken by Member States to safeguard their essential state functions, in particular to safeguard national security, including actions protecting information whose disclosure Member States consider contrary to the essential interests of their security, and to maintain law and order, in particular to facilitate the investigation, detection, and prosecution of criminal offences (Article 2(6)). It should be stressed that it provides for minimum harmonisation, as, under Article 4, Member States may adopt or maintain provisions with a view to achieving a higher level of security of network and information systems.

For the purpose of the NIS Directive (Article 4(1)), "network and information systems" are defined as

(a) electronic-communications networks within the meaning of point (a) of Article 2 of Directive 2002/21/EC
(b) any devices or groups of interconnected or related devices, one or more of which, pursuant to a programme, perform automatic processing of digital data; or
(c) digital data stored, processed, retrieve or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection, and maintenance.

The security of network and information systems is understood as the ability of network and information systems to resist, at a given level of confidence, any action which compromises the availability, authenticity, integrity, or confidentiality of stored or transmitted or processed data, or the related services offered by, or accessible via, those network and information systems (Article 4(2)). The operator of essential services means a public or private entity of a type referred to in Annex II (energy, transport, banking, financial-markets infrastructure, healthcare, water-supply and digital infrastructure). Digital services were specified in Annex III (online marketplace, online search engine, cloud-computing services).

In compliance with the NIS Directive, Member States are obliged to identify the operators which are subject to the Directive within each of the sectors listed in Annex II. It is not required to identify all services, but only those of major significance to social and economic interests, and which could be subjected to significant disruptive effects. The significance of a disruptive effect is determined by taking into account the factors listed in Article 6 of the NIS Directive. These refer to the number of users relying on the service provided by the entity concerned, the dependency of other sectors (referred to in Annex II) on the service provided by that entity, the impact which incidents could have on economic and societal activities or public safety, the relative impact of social and economic interests, market share, geographical spread, etc. Chapter II governs the national frameworks on the security of network and information systems. Article 7 obliges each Member State to adopt a national-security strategy, while at the same time defining the issues to be considered therein. Article 8 obliges each Member State to designate competent authorities on the security of network and information systems (supervising their compliance with the provisions implementing the NIS Directive) and single points of contact. The

Directive provides for establishing computer security incident response teams (CSIRTs) (Article 9) charged with the management of risks and incidents in the sectors defined in Annex II, and in the services listed in Annex III. Furthermore, the NIS Directive provides for cooperation at the national level between competent authorities, single points of contact, and CSIRTs (Article 10). Cooperation between Member States was regulated in Chapter III, which envisages establishing a Cooperation Group (Article 11) composed of representatives of Member States, the Commission, and ENISA, and entrusted with providing strategic guidance for the activities of the CSIRT network, exchanging information and best practices, etc. Article 12 obliges Member States to establish a national CSIRT network, the principal duty of which will be to ensure coordinated response to incidents. The NIS Director provides for certain security and incident-reporting obligations to be imposed both on operators of essential services (Article 14) and on digital service providers (Article 16).[31]

There are numerous documents related to the NIS Directive, including legal Acts of a binding and non-binding character:

1. Commission Implementing Regulation (EU) 2018/151 of the 30th of January 2018 laying down the rules for the application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems, and of the parameters for determining whether an incident has a substantial impact.[32]
2. Commission Implementing Decision (EU) 2017/179 of the 1st of February 2017 laying down the procedural arrangements necessary for the functioning of the Cooperation Group, pursuant to Article 11(5) of Directive (EU) 2016/1148 of the European Parliament and of the Council, concerning measures for a high common level of security of network and information systems across the Union.[33]
3. Communication from the Commission to the European Parliament and the Council: Making the most of NIS—towards the effective implementation of

[31] Savin (2017), pp. 347–348.

[32] Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact, OJ EU 2018 L 26/48.

[33] Commission Implementing Decision (EU) 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5) of the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, OJ EU 2017 L 28/7.

Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.[34]

4. Commission Recommendation (EU) 2017/1584 of the 13th of September 2017 on coordinated responses to large-scale cybersecurity-incidents and crises.[35]
5. Joint Communication to the European Parliament and the Council—Resilience, Deterrence, and Defence: Building strong cybersecurity for the EU.[36]

10 Directive (EU) 2018/1972 Establishing the European Electronic Communications Code

Directive (EU) 2018/1972 of the European Parliament and of the Council of the 11th of December 2018 establishing the European Electronic Communications Code (Recast) (Text with EEA relevance)[37] recast and replaced Directives 2002/19/EC, 2002/20/EC and 2002/21/EC (with subsequent amendments), the provisions of which were meant to be transposed to the legal order of EU Member States by 2003. The new provisions included in Directive (EU) 2018/1972 should be implemented in the legal order of EU Member States by the 21st of December 2020, and will be deemed applicable from that date. The Directive entered into force on the 20th of December 2018.[38]

[34]Communication from the Commission to the European Parliament and the Council: Making the most of NIS—towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union COM(2017) 476 final 2.

[35]Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, OJ EU 2017 L 239/36.

[36]Joint Communication to the European Parliament and the Council—Resilience, Deterrence, and Defence: Building strong cybersecurity for the EU JOIN(2017) 450 final.

[37]Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) Text with EEA relevance. PE/52/2018/REV/1, OJ EU 2018L 321/36.

[38]Article 125 of the Code stipulates that Directives 2002/19/EC [Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on the access to and the interconnection of electronic communications networks and associated facilities (Access Directive) (OJ EC 2002 L 108/7], 2002/20/EC [Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) (OJ EC 2002 L 108/21], 2002/21/EC [Directive 2002/21/EC of the European Parliament and of the Council, of 7 March 2002 on a common regulatory framework for electronic communications networks and services (A Framework Directive) (OJ EC 2002 L 108/33], and 2002/22/EC [Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (OJ EC 2002 L 108/51], listed in Annex XII, Part A, will be repealed on 21 December 2020 without prejudice to the obligations of Member States relating to the time-limits for the transposition into national law and the dates of application of the Directives set out in Annex XII, Part B. Article 5 of Decision 243/2012/UE [Decision No 243/2012/EU of the European Parliament and of the Council of 14 March 2012 establishing a multi-annual radio spectrum policy

Directive 2018/1972 is a set of new or updated solutions regulating activities in the communications sector, i.e. issues pertinent to electronic-communications networks (tele-communications networks), communications services, and associated equipment and services. It also defines the expertise of national regulatory bodies and other responsible entities, and also envisages a range of procedures serving the purpose of harmonising the regulatory frameworks across the EU. Its aim is to promote the internal market in the field of electronic-communications networks and services, e.g. by stimulating competition and increasing investments in 5G and high-capacity networks, leading to the proliferation of such networks, the achievement of sustainable competition, the development of the interoperability of electronic-communications services, accessibility, network and services securing, and the provision of other benefits to end users, so as to ensure that all EU citizens and businesses can use high-quality communications, enjoy a guaranteed high level of consumer protection, and choose from a wide range of innovative digital services. This involves ensuring the provision, throughout the Union, of good-quality, affordable, publicly available services through effective competition and choice, to deal with circumstances in which the needs of end-users, including those with disabilities, in order to access the services on an equal basis with others are not being satisfactorily met by the market, and to lay down the necessary end-user rights (Article 1 (2) of Directive 2018/1972).

In compliance with Directive 2018/1972, national regulatory bodies and other responsible bodies, as well as BEREC,[39] the Commission, and Member States, should seek to attain the following general objectives.

1. To promote connectivity with and access to, and the take-up of, very-high-capacity networks, including fixed, mobile, and wire-less networks, by all citizens and businesses of the Union
2. To promote competition in the provision of electronic-communications networks and associated facilities, including efficient infrastructure-based competition, and in the provision of electronic-communications services and associated services
3. To contribute to the development of the internal market in the field of communications networks and services in the EU by

   (a) removing the existing obstacles to investments in electronic-communications networks, associated facilities and services, and electronic-communications services

programme. Text with EEA relevance (OJ EU 2012 L 81/7)] is removed, effective on 21 December 2020.

[39]The Commission, the Body of European Regulators for Electronic Communications (BEREC) is expected to ensure that EU regulations are complied with in a consistent manner to facilitate the efficient functioning of the single electronic-communications market across the EU. It provides advice to EU institutions, whether at their request or on its own initiative. BEREC includes the so-called regulatory authorities council, which is composed of heads of the national regulatory bodies from each EU Member State (or designated senior representatives of those bodies).

(b) rendering such networks and facilities accessible
(c) providing such services across the Union
(d) facilitating the consolidation of terms and conditions governing investments in such networks, facilities and services, as well as rendering them accessible and ensuring their provision

4. To develop common rules and predictable regulatory approaches as regards

(a) favouring the effective, efficient, and coordinated use of radio spectra
(b) open innovation
(c) the establishment and development of trans-European networks
(d) the provision, availability, and interoperability of pan-European services and end-to-end connectivity

5. To promote the interests of the citizens of the Union by ensuring connectivity and the widespread availability and take-up of very-high-capacity networks, including fixed, mobile, and wire-less networks, and of electronic-communications services by

(a) enabling the generating of maximum benefits in terms of choice, price, and quality, on the basis of effective competition
(b) maintaining the security of networks and services
(c) ensuring a high and common level of protection for end-users through the necessary sector-specific rules, and
(d) addressing the needs—such as affordable prices—of specific social groups, in particular end-users with disabilities, elderly end-users, and end-users with special social needs, and by providing choice and equal access for end-users with disabilities.

Member States were obliged to ensure that entities providing public-communications networks or publicly available electronic-communications services take appropriate and commensurate technical and organisational measures to manage the risks posed to the security of networks and services. These measures must ensure a level of security appropriate to the risk presented, having regard to the state of the art. In particular, measures, including encryption, where appropriate, are required to prevent and minimise the impact of security incidents on users, and on other networks and services (Article 40(1)). The coordination of Member States will be facilitated by ENISA in order to avoid diverging national requirements that might create security risks and barriers to the internal market (Article 40(2)).

11 Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (The European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification, and Repealing Regulation (EU) No 526/2013

Finally, two entities, i.e. the European Agency and the European Cybercrime Centre, are worth mentioning. The European Union Agency for Cybersecurity (ENISA) was set up as The European Network and Information Security Agency on the 15th of March 2004 by way of Regulation (EC) No 460/2004 of the European Parliament and of the Council of the 10th of March 2004 establishing the European Network and Information Security Agency.[40] Its objective is to provide assistance to EU Member States regarding broadly understood cybersecurity issues, and to drive the development of the information society. Under Article 27 of Regulation No 460/2004, the European Network and Information Security Agency was established for a period of five years, starting from the 14th of March 2004. Its duration was then extended twice by way of two subsequent regulations [Regulation No 1007/2008 of the European Parliament and of the Council of the 24th of September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration,[41] and Regulation (EC) No 580/2011 of the European Parliament and of the Council of the 8th of June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration[42]]. Then, the Agency operated under Regulation (EU) No 526/2013 of the European Parliament and of the Council of the 21st of May 2013 concerning the European Union Agency for Network and Information Security (ENISA),and repealing Regulation (EC) No 460/2004,[43] in

[40]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 (Text with EEA relevance), OJ EU 2004 L 77/1.

[41]Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration (Text with EEA relevance), OJ EU 2008 L293/1.

[42]Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration Text with EEA relevance, OJ EU 2011 L 165/3.

[43]Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 Text with EEA relevance, OJ EU 2013 L 165/4.

which its duration was envisaged to continue for seven years. As was rightly noted by C. Banasiński and W. Nowak, this limited duration, even if subsequently extended, significantly reduced the Agency's authority, hindering any long-term planning, and affecting in a negative way the situation of the entities to which its services were addressed. It was also contradictory to the NIS Directive which (see further comments) entrusted the Agency with certain tasks.[44] Regulation (EU) No 2019/881 of the European Parliament and of the Council of the 17th of April 2019 on ENISA (The European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification, and repealing Regulation (EU) No 526/2013,[45] put an end to the temporary character of the Agency. Not only did it envisage the Agency's duration to be unlimited, but it also vested new rights and duties in the Agency (*inter alia*, relating to certification and normalisation).

The Regulation, along with determining the objectives and duties of ENISA, and regulating its organisational matters, provides a framework for the establishment of European cybersecurity certification schemes, for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services, and ICT processes in the Union, as well as for the purpose of preventing the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union (Article 1(1)). The framework provides for a mechanism to establish European cybersecurity certification schemes, and to attest that ICT products, ICT services, and ICT processes, which have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity, or confidentiality of stored or transmitted or processed data, or the functions or services offered by, or accessible via, those products, services, and processes throughout their life cycle (Article 46(2)).

12 The European Cybercrime Centre (EC3)

In turn, the European Cybercrime Centre (EC3) established by way of the Communication from the Commission to the European Parliament, and the Council, "Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre",[46] is in charge of coordinating EU efforts aimed at tackling cybercrime. In addition, it operates as a technical-expertise centre specialising in this field. Its capacities, therefore, overlap with those of ENISA.

[44] Banasiński and Nowak (2018), p. 151.

[45] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), OJ EU 219 L 151/15.

[46] Communication from the Commission to the Council and the European Parliament Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre COM/2012/0140 final.

References

Banasiński C, Nowak W (2018) Europejski i krajowy system cyberbezpieczeństwa. In: Cyberbezpieczeństwo. Zarys wykładu, Warsaw
Chałubińska-Jentkiewicz K (2019) Cyberodpowiedzialność, Toruń
Kuliński M (2010) Regulacje komunikacji elektronicznej, Warsaw
Radoniewicz F (2015) Techniki implementacji do polskiego porządku prawnego postanowień decyzji ramowych Rady Unii Europejskiej dotyczących prawa karnego materialnego, Przegląd Prawa Konstytucyjnego 3
Radoniewicz F (2016) Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym, Warsaw
Radoniewicz F (2017) Ujęcie przestępstw przeciwko ochronie informacji w Kodeksie karnym a postanowienia dyrektywy 2013/40/UE dotyczącej ataków na systemy informatyczne – aspekty wybrane. In: Kitler W, Taczkowska-Olszewska J (eds) Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne, Warszawa
Radoniewicz F (2019a) In: Kitler W, Taczkowska-Olszewska J, Radoniewicz F (eds) Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, Warsaw
Radoniewicz F (2019b) Zwalczanie cybeterroryzmu w prawie UE – aspekty karnomaterialne. Cybersecurity and Law 2
Savin A (2017) EU internet law. Cheltenham–Northampton

Filip Radoniewicz PhD; legal advisor; adjunct in the Department of Cybersecurity Law and New Technologies at the Institute of Law, War Studies University, Warsaw; expert at the Academic Centre for Cybersecurity Policy, (War Studies University) and in the Ministry of Justice; he worked as an assistant judge (in the Fourth Criminal and Sixth Penitentiary Department of the Regional Court in Lublin); graduate of post-graduate studies: "European Union Law" at the Jagiellonian University, "Human Rights and Freedoms", co-organized by the Institute of Legal Sciences of the Polish Academy of Sciences and the Helsinki Foundation for Human Rights, and "Computer Network Administration" at the Lublin University of Technology; author or co-author of approximately fifty publications, mainly in the field of broadly understood criminal law, new technology law and human rights. Selected publications: F. Radoniewicz (2016) Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym / Criminal liability for hacking and other offences against computer data and information systems/, Wolters Kluwer, Warszawa; Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz /Act on the National Cybersecurity System. Commentary/ (2019) ed. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, CH. Beck, Warszawa.