DOI: 10.24193/OJMNE.2022.38.05

LEGAL, POLITICAL AND ORGANIZATIONAL ASPECTS OF CYBERSECURITY IN THE EUROPEAN UNION

Marta GRABOWSKA, PhD
Centre for Europe, University of Warsaw, Poland
mgrabowska@uw.edu.pl

Abstract: *The main objective of the article is to present the development and the current situation with regard to political, legal and organizational aspects of cybersecurity in the European Union. The European Communities entered the information society era later than the US and Japan did. Following the Lisbon Strategy, however, the European Union has been developing it dynamically, and one of the main elements of these activities is cybersecurity. It has been increasingly a crucial point of safety of the whole virtual environment since the rising and such rapid development of information and communications technologies. The article presents a short history of the development of the information, digital and gigabit society in the European Union according to its subsequent long-term strategies, emphasising on the analysis of the development of European Union activities as regards cybersecurity in the political, legislative and organisational aspects. Some Polish threads are included, too. The paper is a result of a longstanding observation by the Author of the development of the information society in the European Union, is based on the EU's official documents, national and international reports, visits, expert studies, and literature on the subject. The study shows that the activities implemented by the European Union are very often of a pioneering character on a world scale, apply system solutions, and are characterised by the logic of the sequence of endeavours made to ensure a high level of cybersecurity in its territory. These seem to be effective as shown by the high position of the European continent in cybersecurity rankings in the world.*

Keywords: Cybersecurity, European Union's activity and legislation on cybersecurity, European Union, Poland.

Introduction

Cybersecurity means to prevent, address and respond to network and information security problems. It means the ability of a network or information system to resist, at a given level of confidence, to accidental events or unlawful and malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and related services offered by or accessible via these networks and systems (*Regulation*, 2004). Cybersecurity is a guarantor of the safety of a digital society and should ensure its proper functioning. To achieve this goal, technical, organizational, legal and political measures must be implemented. We have the bulk of research papers on technical aspects of cybersecurity as new threats come up continuously. This aspect of cybersecurity is a realm of engineering and will not be discussed here. The European Union, however, as a political and economic organization managing a huge common market of 27 Member States which gradually has been becoming digital, has taken serious steps to establish a system of cybersecurity using its main tool, i.e. the European Union's law. This unprecedented cybersecurity system has become a subject of this paper. Thus, firstly, the Council of Europe's and the European Union's official documents on cybersecurity in context of the development of the European information and digital society had been identified and ordered in chronological sequence, then analysed using the method of text analysis. It enabled to draw a picture of the European Union's cybersecurity system which has been built step by step systematically and consistently on both levels: of the European Union and of the Member States to ensure a high quality of digital safety. On this stage of the research systems analysis methodology became useful since the European Union's cybersecurity system consists of many institutions, organizations and networks of which cooperation and mutual relationships are crucial. It can be observed also that the whole structure, particularly in recent times, depends strongly upon political circumstances not only in the European Union but globally, that's why some political context can be noticed in the background. Finally, comparative and statistical data show that although the European Union's cybersecurity system is still under development, however, applied solutions are successful and trailblazing.

Apart from written sources, i.e. the Council of Europe's and the European Union's official documents, reports and the literature on the subject, a longstanding direct observation (international conferences and visits) of the development of the European Union's cybersecurity system in the context of the development of the information, digital, and, latterly gigabit society, became useful.

The concept of cybersecurity is closely linked to the emergence and development of information and communication technologies and the databases, networks, and information systems built based thereon. Poles are attached to the history of these technologies since it has its roots in the achievements of Polish Cryptologists M. Rejewski, J. Różycki, and H. Zygalski. They were the ones who broke the German Enigma code, and a special role was played by engineer J. Ciężki - the fourth member of that group, whose contribution was the use of mathematical methods, not linguistic, as had happened before, to break military codes (Rejewski, 1980; Rejewski, 1981). The Polish cryptologists' discovery then travelled a long way to the United Kingdom, where, at the local decryption centre in Bletchley Park near London, the outstanding British mathematician Alan Turing built the first computer (Hodges, 2014). The technology subsequently made its way to the US, where scientists such as Ralph Hartley, Claude E. Shannon, Warren Weaver, and Norbert Wiener laid the foundations for the development of new disciplines: electronics, computer science, and electronic communications. Based on these sciences, a new type of society emerged, i.e., the information society. It should not be forgotten that there was a Japanese version of Enigma (Japan was Germany's ally during the Second World War). Those who have had the opportunity to visit the British decryption centre at Bletchley Park (Blethley, 2021) could learn about the Japanese Enigma and see the reason why the technology was transferred to Japan.

While in the United States of America, the first applications of new information technologies took place in the military, at universities, and, in the 1960s, in industrial work organisation. In Japan, however, they were mainly used in business and administration. In 1963, Japanese scientist Tadeo Umesao used the term "johoka shakai" for the first time, meaning "a society that communicates with the use of computers". It was also in Japan whereby the Japanese Ministry of Industry and International Trade began implementing programs known as "Technopolis" and "Teletopia", which aimed at connecting several Japanese cities and rural areas with electronic communication networks and transferring the work of administration, business, and citizens to the network (Kitagawa, 2021).

In view of the news about Japanese achievements in building a new type of society, the incumbent president of France, Valery Giskard d'Estain, sent, in 1978, two of his advisers there, whose task was to prepare a report on the application of new information technologies in the Far Eastern country. Their names were Alan Minc and Simon Nora. The comprehensive report they brought home, entitled *L'informatisation de la societe* (Nora, 1978) became the first description of a functioning information society available in Europe.

Europe reacted to these events with delay. Even though Alan Turing's achievements in the United Kingdom had been continued until the early 1950s, the war's destruction of the entire continent and the concentration of efforts and resources on its reconstruction set the issue of new information technologies aside. Europe, in the face of energy shortages and threats resulting from the development of the Cold War, was more interested in nuclear, aviation, and space technologies, and therefore a technological gap between the US and Japan versus the European Communities emerged in the field of information technologies, the aftermath of which is felt to this day. The reason behind it was also the relatively late establishment of research and technological development policy (*Single*, 1987), as well as industrial policy (*Treaty*, 1992) by the European Communities, which hindered the development of information technologies and their implementation in the pan-European dimension. The establishment of the European single market and actions taken in the field of trans-European networks, as well as European standardisation made it just possible to gradually overcome the technical difficulties and lay the foundations for the development of the European information society.

The development of the information, digital and gigabit society in the European Union

In the Brussels administration circles, Jacques Delors was the first to undertake the need to develop the information society in the European Union. His White papers - *Growth, competitiveness, employment. The challenges and ways forward into the 21st century. White paper* (*Growth*, 1993) probably was the first official document which indicated the need to build a new economic strategy for the European Union based on the rapid development of the information society. In a famous report published a year later (*Europe*, 1994; *Resolution*, 1994), Martin Bangemann, the then Telecommunications Commissioner, identified 10 key areas where new information technologies should be implemented first. In 1997, the *Green Paper on the Convergence of the telecommunications, media and information technology sectors and the implications for regulation. Towards an information society approach* (*Green*, 1997), heralded the convergence of all information technologies, and in 1999 the Information Society Directorate General was established. It was the time when the first long-term development strategy of the European Union emerged i.e., the Lisbon Strategy (2000-2010) (*Lisbon*, 2000). Its foundation was the initiative *eEurope - An information society for all* (*Communication*, 1999), implemented in three stages: *eEurope 2002* (*Communication*, 2001) *eEurope 2005* (*Communication*, 2002) and *i2010* (*Communication*, 2005). Although not all objectives of the foregoing stages were achieved during the era of the Lisbon Strategy - most notably the one with regards to catching up with the United States of America and Japan - however significant progress was made in building the European information society and increasing awareness of its role in all activities of the European Union. In 2001, at the meeting of the European Council in Gӧteborg (*Presidency*, 2001), a decision to include 10 associated countries - the then candidates for the European Union membership, of which some were Central and Eastern Europe countries in those activities - was also adopted.[1] In 2005, in view of the increasing digitisation of the media, the name of the Directorate-General was changed to Information Society and Media and there was a clear shift in the terminology used in official documents from "information society" to "digital society". From 1st of July 2012, two Directorates General were created: DG Connect and DG for Communications, Networks Content and Technology.

The subsequent long-term development strategy of the European Union, *Europe 2020* (*Europe*, 2020), which set the three main objectives of smart growth, sustainable growth, and inclusive growth, also focused on the knowledge-based economy, and among the seven flagship projects, *A Digital Agenda for Europe* (adopted on 19 May 2010) directly referred to a digital society (*Communication*, 2010). It set out seven tasks, in particular, building a digital single market and over 100 detailed plans, the majority of which have already been completed. The implementation of these projects was managed by DG Digital Economy and Society, and the advantage of the method of implementing the entire *Europe 2020* strategy was the establishment of a monitoring mechanism in the form of the European Semester by the European Commission. It disciplined the Member States in implementing the set objectives and tasks. The Lisbon Strategy lacked such a mechanism. However, nowadays the EU average for the development of digital society in the world according to the I-DESI Index (International Digital Economy and Society Index) (*European*, 2021), which compares the European Union as a whole (EU-27) against other selected countries in the world in terms of the information society development,

[1] "Taking account of their particular situations, candidate countries are invited to translate the Union's economic, social, and environmental objectives into their national policies. The intention of candidate countries to adopt the eEurope+ initiative is a successful example. Starting from Spring 2003, the Commission will begin covering the candidate countries and their national policies in its annual synthesis report" p.2.

still places the EU at a lower level than the USA and Japan, even though some highly developed EU countries such as Finland, Sweden, the Netherlands, and Denmark meet the index criteria.

There is a new financial framework for the years 2021-202. The fundamental direction to be pursued has not changed. Leading further developments of the European Union towards digitisation and data economy is crucial. In view of the next technological leap of the 21st century and the emergence of an array of new information technologies such as Internet of Things (IoT), Big Data Analytics, Artificial Intelligence, Cloud Computing, Robotics, 5G internet, virtual and augmented reality, supercomputers, etc., the European Union faces a new challenge in building a European gigabit society (Grabowska, 2020).

Cybersecurity in the European Union during the Lisbon Strategy (2000-2010)

Cybersecurity in the development of the information society in the European Union has already appeared in a communication from the European Commission *Network and Information Security: Proposal for A European Policy Approach* (*Network*, 2001) and in the Council Resolution of 28 January 2002 (*Council*, 2002). However, a specific action plan was established only at the second stage of the implementation of the aforementioned *eEurope - An information society for all* initiative (*Communication*, 1999), which constituted the basis for the Lisbon Strategy. It was *the eEurope 2005 Action Plan* (*Communication*, 2002), whose objectives for the years 2003-2005 were adopted in Seville in June 2002. The plan indicated four key areas that should undergo prompt computerisation, i.e., eBusiness, eGovernment, eHealth, and eLearning. The need to build broadband connectivity in the European Union and to **ensure the cybersecurity** of the entire infrastructure indispensable to implement the plan was also emphasised. It was agreed that the infrastructure should be subject to constant security monitoring.

The most important achievement of the said objectives was the establishment of the European Union Agency for Network and Information Security in 2004 (ENISA) (*Regulation*, 2004) based in Heraklion, Crete (Greece). The Agency's task was to monitor the security of the entire EU information infrastructure, i.e., data transmission networks (cables, internet, radio waves, optical and magnetic carriers, satellite transmission, terrestrial networks, mobile telephony networks, etc.), as well as overseeing information systems using computers, electronic communication, and digital data.

Undesirable phenomena in the digital world are consistent with two basic violations, i.e., technical infrastructure and social behaviour. These phenomena are called **incidents**. They can lead to intentional or unintentional crisis situations consisting of damage to technical infrastructure, improper use thereof, or even its complete disablement and destruction. They can also lead to harm to people as a consequence of using inappropriate content, which can result in the violation of human rights, the conducting of illegal activities including the theft of data or property, as well as conducting illegal commercial or terrorist activities. (Furnel, 2002)

The first mass cyber-attacks occurred in the USA in the late 1980s. Therefore, in 1988, at Carnegie Mellon University (Pittsburgh, Pennsylvania), the first group of specialists emerged under the name of the Computer Emergency Response Team (CERT) (Carnegie, 2021), which, being available 24/7, accepted incident reports in order to recognise and remove them. The idea of CERT spread around the world, including European Union countries, and to this day many CERT centres conduct such activities. There is also CERT-EU (CERT-EU, 2021) as well as CERT.PL (NASK, 2021). Anyone can report an incident there, even anonymously. The team’s assistance is especially convenient at the national level. There are also specialised CERT teams working specifically for particular institutions, enterprises, or organisations.

Detecting and investigating incidents, however, does not put an end to a case. Database and information systems security is often insufficient. The main issue is to legislate and organise law enforcement and the judiciary in such a way that, once an incident is identified, it is possible to apprehend the perpetrators and bring them to justice.

The first piece of legislation on cybercrime in Europe was the Council of Europe’s Convention adopted on 23 November 2001 in Budapest entitled the *Convention on Cybercrime* (Council, 2001) with ETS no. 185 and the European Court of Human Rights in Strasbourg as a judicial institution. The convention became the first international legal act investigating crimes committed in and with the use of computer systems, including *inter alia* violating the security of networks and computer systems, hijacking network information content, computer fraud, child pornography, or the violation of copyright. Although the Council of Europe’s Conventions, apart from *The Convention for the Protection of Human Rights and Fundamental Freedom* (Council, 1950), are acts that may be applied voluntarily, their ratification, however, implies the obligation to implement the content of the convention into national legislation. These conventions can also be ratified by non-member states of the Council of Europe. Among its Member, *Convention on Cybercrime* has not yet been ratified by Ireland (it plans to ratify the Convention in the nearest future) and the Russian Federation.

Poland ratified it after a long delay, in 2015, explaining that the delay was due to the preparations of relevant law enforcement and judicial authorities. Amongst the non-member states of the Council of Europe, the Convention has been ratified, for example, by the United States of America and Australia, but not by China. The Convention set the reference framework for the first works on European Union legislation in that field. These include *Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems* (*Council*, 2005) and the D*irective 2013/40/EU of the European Parliament and of the Council of August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA* (*Directive*, 2013). The foregoing documents addressed to the Member States indicated the need to take effective action in the harmonisation of criminal law as regards cybercrime, the establishment of law enforcement agencies, as well as the approximation of legal systems in that field. "Without right" conduct was defined there as "access, interference, or interception, which is not authorised by the owner or by another right holder of the system or a part of it, or not permitted under national law" (*Directive*, 2013). Member States were required to establish a network of 24/7 national contact points for the efficient prosecution and information exchange on cybercrime.

Cybersecurity in the era of the *Europe 2020 Strategy*

With the advent of the new multi-annual development strategy of the European Union, E*urope 2020* (*Europe*, 2020), the importance of cybersecurity increased. With a view to implement the objectives set out in *A Digital Agenda for Europe* (*Communication*, 2010), i.e. one of the 7 flagship projects of the *Europe 2020* strategy covering the issues of digitisation, including the development of the digital single market, interoperability of devices, databases and applications, completion of works related to the public administration and health sector digitisation, the development of electronic commerce and banking, and mobile telephony, as well as the urgent need to create a new generation network and increase the ICT potential in the

European Union, decisions to double the expenditure on research and innovation in the ICT sector and to strengthen **networks trust and security** were made.

For example, in electronic administration, and, in particular, in electronic public services, the secure electronic identification of citizens plays an important role. The European Communities launched the eID (electronic identification of citizens) and eIDAS (electronic identification of citizens for public administration) programs (*Regulation*, 2014). The European Commission assumed control of the electronic identification of citizens by gaining the exclusive right to designate units at the national level, which subsequently have the exclusive right to grant licenses and certificates to institutions and businesses in each country specialising in the creation of trusted profiles and electronic signatures. The units designated by the European Commission for these activities in the Member States are most frequently national banks, and this is also the case in Poland. It is the National Bank of Poland, namely The National Certification Centre (NCCert) operating at the Bank that, in the field of trust services and electronic identification (National, 2021), grants licenses and certificates to service providers and oversees the electronic identification system of citizens. In electronic systems of public services (in Poland it is the Electronic Platform of Public Services) (ePUAP, 2021), the so-called Trusted Profile is used, which is a type of electronic signature, solely effective on this platform. As opposed to a trusted profile, a qualified electronic signature is effective in any situation and has the power of a handwritten signature, mainly in the area of the digital single market. Both in eGovernment and in the business area, the following tools can also be identified: an electronic seal, electronic time stamp, website authentication, and electronic official delivery confirmation. Pursuant to EU legislation, these tools must also have certificates of the above-mentioned procedures and these actions should have been implemented in the Member States by 1 July 2020 (*Regulation*, 2014). Their service providers are required to use certain ciphers. The European Commission provides a platform encompassing all EU Member States, where one can check whether the foregoing electronic identification tools come from a legal source (CEF Digital, 2021).

Biometric data (fingerprints, facial images, the iris of the eye, or the vascular pattern of the hand) are specific instruments for identifying citizens. They are used more and more often, for example, in mobile phone systems, at border crossing points, in identity documents, etc. Biometric data could also be useful, in e-Voting procedures. However, due to difficulties with e-Voting (Park, 2021) and particularly in collecting this type of data from those entitled to vote (the system must have data for comparison) and the costs associated with the installation of appropriate devices – so far this technology is still under development. Biometric data are successfully used rather with regard to specific groups of citizens only (e.g. passports or ID card holders who provided their biometric data when applying for them). The protection of personal data in IT systems is also a subject of particular concern for the Council of Europe since they are protected by the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* of 28 January 1981 (Council, 1981) and the European Union law by means of the GDPR provisions (*Regulation*, 2016).

On 6 July 2016, another directive was adopted - *Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union* (*Directive*, 2016), which, in facing rapid acceleration in the area of digitisation, constitutes the beginning of new, comprehensive legislative activities of the European Union in cybersecurity. The NIS Directive (Network Information Service) replaced the above-mentioned Directive of 2013 (*Directive* 2013). Its main objective is to guarantee digital security of the so-called critical infrastructure in the Member States, the proper operation of which depends on networks and information systems. Critical infrastructure encompasses the following sectors: energy, transport, banking, financial markets, healthcare, potable water supply and distribution, as well as digital infrastructure supporting these sectors. Unfortunately, an increasing number of attacks on critical infrastructure in various regions of the world has been noted lately. Each EU Member State was obligated to draw up a list of Operators of Essential Services (OESs) and Digital Service Providers (DSPs), i.e., public or private entities providing services within the foregoing sectors. It should be noted that these services may be provided in one or more EU states by operators and suppliers from Member States, or they may be provided by operators and suppliers from outside the EU; in the latter case the provider's representative must register its activity in the European Union. Each Member State was obligated to establish national security strategies for their network and information systems, in particular those providing services in critical infrastructure sectors, i.e. designating competent national authorities for the security of network and information systems, designating a national single point of contact for the security of network and information systems in order to ensure cross-border cooperation and establish cooperation with law enforcement and national data protection authorities. As part of the digital infrastructure, the procedures for the supply of DNS (Domain Name System – hierarchical and decentralised internet domain naming system) services, entities managing TLDs (Top-Level Domains) and IXP network objects (Internet Exchange Points) enabling connections between more than two autonomous systems, are subject to mandatory checks. The following three categories of digital services are also subject to security requirements: online marketplaces, search engines, and cloud computing services. The Directive also obligates Member States to establish one or more Computer Security Incident Response Teams (CSIRT), which form a network (The Network of CSIRT's) coordinated by ENISA in the European Union. Its task is to cooperate with national, European, and international law enforcement agencies including Eurojust, Europol, or the European Cybercrime Centre (ECC) (Europol, 2021) established within Europol, in order to mainly combat cross-border incidents and, along with other institutions and international organisations, i.e. NATO and the OSCE, to ensure cybersecurity. Operators of essential services and digital service providers should immediately (within 24 hours) report to CSIRTs centres incidents that could jeopardise the continuity of service provision. Such reports should include, *inter alia*, information on the number of users affected by the incident, its geographic scope, and the projected ramifications of the incident. The legal provision also provides for the need to inform the public about the incident, should it be justified. At the EU level, the Support Group was launched to monitor and analyse the activities of the CSIRTs network in order to exchange good practices and set strategic goals.

In connection with the NIS Directive, Poland adopted *the Act of 5 July 2018 on the national cybersecurity system* (*Ustawa*, 2018) as the first legal act in our country regulating that matter. The cybersecurity management scheme adopted in *the Act* is fairly complicated: the "Cybersecurity Strategy" is adopted by the Council of Ministers by way of a resolution, the cybersecurity competent authorities are the ministers of individual ministries listed in *the Act*, the coordination of activities and implementation of the government's cybersecurity policy is entrusted with a plenipotentiary, appointed and dismissed by the Prime Minister, and a Council at the Council of Ministers which acts as a consultative and advisory body on cybersecurity. The minister responsible for computerisation, following the Ministry of Digitisation's decommission on 7 October 2020 in relation with government reconstruction, is currently located in the Chancellery of the Prime Minister, acting as the Secretary of State, Government Plenipotentiary for Cybersecurity. This official prepares a "Strategy" together with ministers, and following its adoption by the Council of Ministers, submits it to the European Commission, with which it cooperates and, *inter alia*, runs a Single Point of Contact. Currently, the Cybersecurity Strategy for 2019-2024 (*Uchwała*, 2019; Ministry, 2019) is being implemented in Poland, and was prepared at the Ministry of Digitisation and adopted by the Council of Ministers on 22 October 2019. On the basis of *the Act*, three Computer Security Incident Response Teams were established in Poland, namely: CSIRT.GOV, run by the Internal Security Agency (ABW) under the supervision of the Government Plenipotentiary for Cybersecurity (CSIRT, GOV, 2021), CSIRT.MON, run directly by the Ministry of National Defence (MON) (CSIRT, MON, 2021), and CSIRT.NASK, run by the Scientific and Academic Computer Network - National Research Institute (CSIRT.NASK, 2021). The latter also encompasses the aforementioned CERT.PL centre, which has been operational since 1996 and supported the general public in dealing with incidents and implementing a number of cybersecurity projects that allow for the forecast of threats in IT infrastructure systems of central and local government offices. It examines also the security of protected locations. *The Act* came into force at the end of 2018. It should be added that Poland is not among the leaders in the fight against cybercrime, yet the number of cyber-attacks is not insignificant, therefore the need to promptly implement the EU Directive will certainly accelerate Polish activities in that regard.

Other technological leaps in ICT, took place at the beginning of the 21st century, and pointed to the emergence of a number new technologies, such as: Cloud Computing, Big Data Analytics, augmented and virtual reality, artificial intelligence, robotics, the internet of things, industry 4.0., and the next-generation electronic communications network (5G) - indispensable in the face of the rapidly increasing number of devices that will be connected to the Internet. They all has made cybersecurity ever more difficult. Another strategic EU cybersecurity solution is the introduction of certification of devices, software and digital services throughout the entire European Union. Certification is a strictly defined procedure in which an authorised third party (e.g., a specialised laboratory), as a result of an agreed procedure, issues a certificate stating that a product, service or process meets certain compliance conditions, most often with certain standards or technical specifications. And it is precisely what the new *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) No526/2013 (Cybersecurity Act) (Text with EEA relevance)* (*Regulation*, 2019) requires. This Regulation is known as *the Cybersecurity Act*.

It should be remembered that the European Union has initiated certification activities in various areas for a long time. A positive result of the certification process conducted by the European Union authorises a product manufacturer, service provider or process organiser to apply the widely-recognised CE marking. Pursuant to the Regulation, cybersecurity is included into this process. This task is entrusted to ENISA, whose name and organisational structure have changed under the Regulation (now it is the European Union Agency for Cybersecurity)[2], and which becomes the EU's cybersecurity centre. The Regulation states that ICT products, services, and processes related to the critical infrastructure sectors listed in the abovementioned Directive will be subject to certification first.

The task, however, is complex mainly because in order to issue certificates, uniform European standards and technical specifications must be in place in a given area, and, in a number of cases, they should also comply with the relevant international standards. The European Union has a sizeable output in standardisation implemented by the European standardisation organisations, namely CEN, CENELEC and ETSI. However, in the new area of cybersecurity, it will be necessary to begin with establishing EU assurance levels for ICT products, services, and processes, and developing the concept of a European cybersecurity certificate, respectively. Subsequently, once the relevant standards and technical specifications have been adopted, it will be necessary to appoint national accreditation bodies, entities assessing compliance with EU requirements, as well as to adopt principles of conformity assessment. Due to the rapid development of ICT, these activities will be continuous. The Regulation, therefore, establishes a European framework as the basis for cybersecurity certification with the aim of creating a single market for ICT products, services, and processes that meet specific cybersecurity requirements throughout their entire life cycle. The European Commission is preparing a Union rolling work program for European cybersecurity certification, and, as part thereof publishing lists of ICT products, services and processes that will be covered by the European certification procedure. ENISA was obligated to develop relevant legal provisions in that regard, coordinate national cybersecurity certification programs and run a website on the

[2] The acronym ENISA remains unchanged.

European cybersecurity certification program. Individual Member States as well as various private organisations have previously implemented ICT certification initiatives, but they had a local effect only, and these certificates were not always interchangeable. The level of cybersecurity also varies in individual Member States. The EU's objective is to introduce uniform European certificates for ICT products, services, and processes, which will significantly facilitate the interoperability of information systems and increase their security at large.

The Regulation adopted three so-called European assurance levels in ICT products, services, and processes, 1. basic, 2. substantial, and 3. high. Within each level, procedures for granting European certificates corresponding to the forecast risks of their application have been established. The 'basic' level is reduced to a review of technical documentation, including design documentation, by a body assessing compliance with European cybersecurity requirements in order to determine the absence of vulnerabilities of a given ICT product, service, or process to cyber-attacks known as 'basic'. At the 'substantial' level, in addition to meeting the requirements of the 'basic' level, the ICT product, service, or process should be subject to a security functionality test in accordance with the adopted requirements, thereby limiting cyber-attacks carried out by people with limited skills and resources. The 'high' level, however, encompasses - in addition to meeting the requirements of the 'substantial' level - effectiveness tests confirming the proper implementation of modern security functionalities for advanced cyber-attacks carried out by people with significant skills and resources. "Conformity self-assessment" is also recommended, i.e., assessment by the manufacturer or supplier themselves, which is currently recommended under cyber-hygiene. The manufacturer or supplier should prove that ICT products, services, or processes incorporate the indispensable elements of cybersecurity in their concept (design). However, "conformity self-assessment" by a manufacturer or supplier, and not by an assessment body, can only be regarded as 'basic'. In such cases, manufacturers and suppliers also assume full responsibility for their statements and the consequences resulting therefrom. Pursuant to the Regulation, cybersecurity certification in the European Union will be voluntary for the time being, but with regard to specific ICT products, services, or processes, it may become mandatory.

All these activities lead to the gradual regulation of the European market of ICT products, services, and processes with regard to cybersecurity, i.e. control of introducing as well as the safety degree of IT infrastructure elements introduced to the European Union. This is extremely important from the vantage point of each Member State and the entire European Union, especially in regard to critical infrastructure which is not effectively protected these days, and is especially visible, for example, in the progressive convergence of operational technologies (OP) and information technologies (IT), i.e. the collaboration of production processes with IT support (combining industrial automation and IT) (Fournaris, 2018). Due to the rapidly advancing computerisation process in various sectors of the economy, vulnerabilities arise at the intersection of these two technologies which can be exploited by cybercriminals. Industroyer malware can act as an example which, in 2016, cut one fifth of Kiev, Ukraine, off from the electricity grid for an hour (Dragos, Inc., 2021) and similar crimes in other parts of the world. Banking systems and cloud solutions also have gaps. The number of attacks on research centres' resources, government agencies, or military facilities, as well as on various network-connected devices (computers, mobile phones, etc.), has become rampant. The situation was exacerbated during the COVID-19 pandemic, when more camera images, data, and various new applications appeared on the net, which betrayed the fact that the IT environment is not secure. The European Union implements such sensitive solutions as smart homes, cities, or unmanned transportation, and they all have to be safe and secure. ICT products, services and processes certificates will be issued for a specified period of time, after which their re-certification will be required. A European cybersecurity certificate issued in one Member State will be valid in the entire European Union. The Regulation also establishes The European Cybersecurity Certification Group (ECCG), which encompasses representatives of national cybersecurity certification authorities. The Group is chaired by the European Commission with the support of ENISA. The key provisions of the Regulation will enter into force on 28 June 2021.

Pursuant to the requirements of the Regulation in question, ENISA has already launched a website on cybersecurity certification (European, 2021) and a preliminary draft of the procedure in that regard has been developed, which is currently subject to public consultation. It is included in *the Cybersecurity Certification document. EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS*[3] (European, 2020). At the

[3] "The SOG-IS agreement was produced in response to the EU Council Decision of 31 March 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of 7 April (1995/144/EC) on common information technology security evaluation criteria." SOG-IS - Home (sogis.eu) (accessed 25/04/2021)

beginning of 2021, the European Commission also requested ENISA to prepare the candidate cybersecurity certification scheme on 5G networks (European, 2021), compliant with the Regulation in question. ECCG, a group representing the NIS directive, representatives of European standardisation organisations, and experts in the field of 5G technology will be invited to collaborate. Taking such actions in view of the crucial role of the 5G network for the development of the European digital economy means introducing a thorough security check of the entire infrastructure of this network in the European Union. It should be added that some European countries have already taken steps to protect their national 5G networks, such as the United Kingdom, which in July 2020 decided to remove all Huawei devices from its network by 2027 (GOV.UK, 2020), or Sweden, which ordered similar actions in relation to Huawei and ZTE by 2025 (CNBC, 2020). One has to mention that China has not ratified the European *Convention on Cybercrime* (Council, 2001). The introduction of ICT devices, services, and processes certification in the European Union will certainly increase the level of cybersecurity. In Poland, national cybersecurity certification services have already been provided by NASK in collaboration with national laboratories in Warsaw and Katowice, and once the Regulation (EU) 2019.881 enters into force, they will be continued there.

Cybersecurity in the new development perspective of the European Union for 2021-2027

We are currently witnessing the efforts of the European Union related to the ratification of the new development perspective for 2021-2027. There are two funding sources in that perspective: the Multiannual Financial Framework 2021-2027 (NFF) and Next Generation EU (NGEU). A part of it is *Digital Europe* with a fund of 7.5 billion euros (in current prices), mainly from the MFF under the general Single Market Innovation and Digital program. A total of 143.4 billion euros was allocated to the latter (European, 2021). The main objectives of *the Digital Europe* are the development of supercomputers, artificial intelligence, **cybersecurity level enhancement**, digital skills, and the strengthening of eGovernment in the European Union, as well as improving the interoperability of systems. 2 billion euros have been earmarked for cybersecurity. The following objectives in that regard were listed: cybersecurity of the European industry, financing the latest cybersecurity infrastructure, and acquiring relevant skills and knowledge in the field. The new term "cyber defence" emerges as a much broader term compared to the already-used "cyber security" one: it means combating threats not only by reacting to incidents in the network, but also by building mission assurance. Such activities encompass comprehensive threat forecast and their proactive prevention in accordance with our values. The term "proactive" means taking the initiative and intentionally acting in advance, thus enabling the achievement of specific objectives in line with the adopted values. The opposite is, of course, the word "reactive", meaning, in a way, "let things happen" and reacting afterwards. The term "cyber defence" applies not only to the reactive protection of governmental, corporate, and other bodies within the European Union, but also refers to possible threats from outside especially when we are already living in the age of hybrid warfare (cyberwarfare) In this approach, the term "cyber defence" means shifting the burden of responsibility to a greater extent to the power of the country, and, if necessary, to the military spheres in order to maintain security in cyberspace. Examples of such activity in the European Union include *Commission Recommendation (EU 2019/534 of 26 March 2019 Cybersecurity of 5G networks* (*Commission*, 2019), which recommended advance actions in the area of 5G network security, and is expected to underpin the development of digital economy in the European Union, or, the *Prague Proposals* adopted on 3 May 2019 in Prague (the Czech Republic) in cooperation with the USA, whereby Prime Minister of the Czech Republic A. Babiš said: "We need to get 5G right and show responsibility to our citizens and companies alike. 5G is not a one-time business competition. It is a process, where cybersecurity must be a priority from the outset" (Hartman, 2019). NATO's activities also fall into this model of operation in cybersecurity.

However, a major breakthrough in cybersecurity may happen very soon with the development of new information technologies, i.e., quantum technology and optical communication. These technologies can guarantee ultra-secure communications, otherwise referred to as Quantum Internet, throughout the entire European Union, especially in long-distance data transmission, providing quantum computers are connected to satellite systems. Quantum computing was developed on the grounds of quantum physics and engineering, as a result of which quantum computers were created. The term "quantum computing" was forged by American physicist P. A. Benioff as a result of a new approach to information science (information theory) that is quantum information. He proposed the quantum model of the Turing machine (Benioff, 1980). The theory uses a unit called a qubit, i.e., a quantum bit, which is the smallest and indivisible unit of quantum information (as a ‘bit’ is in traditional information theory). A qubit, however, is spatial, which makes it possible to appear in a superposition of any two quantum states, and between these states there is quantum entanglement. It allows one to determine information about the state of one of them knowing the state of the other without the need to measure the former and without the need to send information about the latter. A superposition, therefore, is a list of states and the probability that an object (e.g., a photon) is in a certain state. The selection of one of these states automatically determines the other. An important element of this reasoning is the fact that a specific state, which may be changeable, is not determined but probable. Quantum computers using the principles of quantum mechanics are indispensable for the analysis, processing and transmission of information comprehended in this way. This means that in addition to the traditional values of 0 and 1, as is the case in classical computing, these computers allow you to manipulate intermediate states and make a variable selection of one of them. Their computing power must therefore be much greater. A qubit can store and carry significantly more information than a bit, therefore the qubit is more efficient. Quantum computers in cooperation with satellite systems can create Quantum Communications Infrastructure (QCI), which, together with the Quantum Key Distribution (QKD) cryptographic technology, can constitute ultra-secure communications used, for example, in the exchange of sensitive data between governments and research laboratories, and is indispensable in industry 4.0, smart cities, unmanned transportation, etc. Any attempt to intercept an entangled state modifies the entire system, thus revealing an attempted break-in (Furnkranz, 2020). If, in addition, there is direct contact between two parties involved in the information process, excluding the participation of any third party (such as in blockchain technology), that may be the super-secure internet. Quantum technology has other applications as well, e.g., in medicine, biotechnology, metrology or simulations of complex systems, which, due to the possibility of applying superposition to the latter, may take our imagination even further, i.e., towards ... teleportation (Furusawa, 2011).

In 2019, the EU project Quantum Flagship was launched, for which over 1 billion euros was earmarked, and its implementation has been scheduled for 10 years (European, 2021). The project brings together groups of scientists, industries, entrepreneurs, and politicians, and it is one of the most ambitious future endeavours of the European Union. The initiative was taken by Spain and six other European Union member states. Later, other member states joined in. Pursuant to *the Digital Europe*'s objectives, the project will be continued in the current development perspective of the European Union. The application of quantum technology in cybersecurity may be profitable due to the fact that the costs incurred in the fight against cybercrime and the damage caused thereby can be reduced, and the security of data and information can be guaranteed.

Threat monitoring

There is a number of cyberspace threat monitoring centres. The literature on cyber threats offers various categories of these phenomena, ranging from massive attacks on an international scale to minor ones, such as, the breaking into government bases of different countries or international organisations, election interference, the penetration of banking systems, disrupting the operation of critical infrastructure systems, extorting information from individual citizens, etc. The following are also somewhat significant: lack of attention, ignorance and human gullibility, as well as inadequately secured equipment and ICT links. The implementation of extensive legislation in combating cybercrime does not obviously guarantee the elimination thereof, just as the implementation of criminal law has not and will not eliminate crime. At present, the CSIRT centres in the EU Member States conduct constant monitoring of cybercrimes and issue a warning against any detected trends. Up-to-date reports, analyses, and alerts can be found on those centres' websites. It is worth emphasising that there is already at least one CSIRT (CERT) in every country of the European Union, where an ordinary citizen can report an incident that caused damage to digital ecosystem or any spotted threats. Specialists employed in those centres will conduct an analysis, find a solution, and in some situations refer the case to law enforcement agencies. Due to the fact that information technologies currently represent a very advanced level of development, and an average citizen is not equipped with sufficient knowledge to effectively recognise and overcome a threat or harm, it is best to use the help of these specialists. The problem, however, is that there is little knowledge of these publicly available services among citizens, so they need to be disseminated. In Poland these services are provided by CSIRT.NASK (CSIRT.NASK, 2021). The incident reporting form available there is simple and requires only the incident to be described. There is also a possibility to report by SMS. In life threatening events (e.g., resulting from terrorist activities on the Internet), there is a path to be followed in a critical situation. NASK publishes annual reports *The Security Landscape of the Polish Internet*; the latest report published for 2019 (NASK, 2019) registered over 6,000 incidents, a significant growth compared to previous years. The most common incidents are phishing, malware, offensive and illegal content including spam, a growing number of ransomware infections, bomb threats targeting schools, hospitals and offices, etc. Detailed analyses of individual phenomena are also published, which constitute valuable educational material.

FIRST - Forum on Incident Response and Security Teams (FIRST, 2021) is a global forum for monitoring, analysis, information exchange, and the prevention of cyberthreats reported from various places and regions of the world. This organisation was established in 1989. At present, FIRST has 570 members (5 of whom are from Poland) and they all cooperate in the field of cybersecurity on a global scale.

In turn, ITU - International Telecommunication Union - runs the Global Cybersecurity Index (GCI), under which it publishes cybersecurity assessments of individual countries pursuant to five criteria: 1. legal measures (cybercrime, cybersecurity and spam reduction legislation), 2. technical measures (the functioning of CERT/CSIRT bodies, the application of standardisation in cybersecurity, the use of cloud computing for combating cybercrime, mechanisms for protecting children against cybercrime, technical mechanisms for limiting spam), 3. organisational measures (national cybersecurity strategy and national institutions supervising the implementation of this strategy and cybersecurity monitoring and assessing mechanisms), 4. capacity building measures (building public cybersecurity awareness, organising academic courses and other educational programs in the field, having an accreditation system for cybersecurity specialists, implementing research programs, building incentive systems encouraging raising the level of cybersecurity in the country), 5. cooperation measures (bilateral and multilateral agreements in cybersecurity cooperation, participation in international organisations and forums dealing with cybersecurity, functioning mechanisms of public-private partnership and cooperation of various stakeholders, as well as implementation of good practices). , A general cybersecurity assessment of individual countries and regions of the world is then presented.

The last report for 2018 published in 2019 (International, 2019), shows that in the category of individual countries, out of the 175 listed, the highest scorers are: the United

Kingdom, United States of America, France, Lithuania, Estonia, and Singapore. Subsequently, Japan is 14th, Germany is 22nd, the Russian Federation is 26th, China is 27th, and Poland is 29th. Hungary took 31st and India 47th place. The most distant European Union’s Member State on the list is Malta on 82nd position. Considering all the above-mentioned indicators according to this report, the European continent unquestionably leads in individual indicators as well as in the overall assessment of world regions. The summary of the report even points to the impressive leap that has been made on the European continent in improving the level of cybersecurity. The consistent policy of the European Union in combating cybercrime as well as EU’s support of the process of equalising the cybersecurity level by means of legal, financial, standardisation, and organisational instruments throughout its territory have undoubtedly impacted upon progress.

Conclusions

Cybersecurity in the European Union is an important element of its functioning. Even though the Community entered the era of information society development with a certain delay as compared to the United States or Japan, its activities in that regard have significantly accelerated, starting with the Lisbon Strategy. The development of the information society, and, subsequently, the digital society, has also underpinned the following multi-annual strategies of the European Union, i.e., *Europe 2020* and, the new perspective for 2021-2027. Cybersecurity has been an important element of these activities in recent years. Examining the stages of cybersecurity improvement as a fundamental element in the functioning of the EU's information and digital society proves that these activities constitute a strategic and logical sequence of decisions which have placed this part of the world in first place when it comes to digital security. Establishing ENISA, creating a network of CERT/CSIRT centres, activities aimed at ensuring the security of the EU's critical infrastructure, standardisation and certification of IT devices, services and processes as well as legislative activities in the field of human rights, personal data and intellectual property, facilitating law enforcement and justice systems operation, and finally ensuring cybersecurity level equality in the member states – all these stand for exceptional legal and organisational achievements of the European Union in the field of combating cybercrime. The fight, however, is not over yet, but teamwork offers a better chance of winning.

References:

1. Benioff P. (1980) *The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines,* In: *Journal of Statistical Physics*, vol. 22, issue 5 p. 563-591.
2. Blethley (2021) Park, Bletchley Park | Home (access 26.07.2021).
3. Carnegie (2021) Mellon University. Software Engineering Institute. CERT Division The CERT Division | Software Engineering Institute (cmu.edu) (access 23.07.2021).
4. CEF Digital (2021) Connecting Europe. Trusted List Browser. Tool to browse the national eIDAS. Trusted List and the EU List of eIDAS Trusted List (LOTL) Trusted List Browser (europa.eu) (accessed 02/05/2021) (access 23.07.2021).
5. CERT-EU (2021) CERT-EU News Monitor (europa.eu) (access 02.07.2021).
6. CNBC (2020) Tech : *Sweden bans Huawei , ZTE from upcoming 5G networks*, 20 October 2020 Sweden bans Huawei, ZTE from upcoming 5G networks (cnbc.com) (access 20.07.2021).
7. *Communication* (2019) *Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks*. OJ L 88, 29.3.2019, p. 42–47.
8. *Communication* (1999) *of 8 December 1999 on a Commission initiative for the special European Council of Lisbon, 23 and 24 March 2000 - eEurope - An information society for all* [COM (1999) 687 final – not published in the *Official Journal*] EUR-Lex - l24221 - EN - EUR-Lex (europa.eu) (access 25.07./2021).
9. *Communication* (2001) *from the Commission of 13 March 2001 - eEurope 2002: Impact and Priorities, a communication to the Spring European Council in Stockholm, 23-24 March 2001* [COM (2001) 140 final - not published in the *Official Journal*] (accessed 02/05/2021) EUR-Lex - l24221 - EN - EUR-Lex (europa.eu) (access 02.07.2021).
10. *Communication* (2002) *from the Commission of 28 May 2002 – eEurope 2005 Action Plan: An information society for all* [COM(2002) final – not published in the *Official Journal*]. EUR-Lex - l24221 - EN - EUR-Lex (europa.eu) (access 02.07.2021).
11. *Communication* (2005) *from the Commission of 1 June 2005 – "i2010" – A European Information Society for growth and employment"* [COM(2005)229 final – not published in the *Official Journal*] EUR-Lex - l24221 - EN - EUR-Lex (europa.eu) (access 02.07.2021).

12. *Communication* (2010) *from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, A Digital Agenda for Europe*. COM/2010/0245 final.

13. Council (1950) of Europe. *Convention for the Protection of Human Rights and Fundamental Freedoms*. Treaty no. 005. Rome 4/11/1950.

14. Council (1981) of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* from 28 January 1981. Treaty no. 108.

15. Council (2001) of Europe, *Convention on Cybercrime*. Treaty no. 185. Budapest, 23/11/2001.

16. *Council* (2002) *Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information society* (2002/C 43/02) OJ C/43 from 16 February 2002, p. 3-4. http://scan.lex.pl/unia/2002/32002g0216(02).pdf?&_ga=2.108074250.905615166.1619625032-1124450630.1614434229#xd_co_f=Nm (access 24.04./2021).

17. *Council* (2005) *Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems*. OJ L 69, 16.3.2005, p. 67–71.

18. CSIRT. GOV (2021) Computer Security Incident Response Team CSIRT GOV (access 02.07.2021)..

19. CSIRT.MON (2021) of the Ministry of National Defence/ CSIRT MON (wp.mil.pl) (accessed 23.07.2021).

20. CSIRT.NASK (2021) CSIRT NASK - NASK (access 23.07.2021).

21. Directive (2013*) 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 L 218, 14.8.2013, p. 8–14.

22. Directive (2016) (*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 L 194, 19.7.2016, p. 1–30.

23. DRAGOS. Inc. (2017) *Crashoverride: Analysing the Malware that Attacks Power Grids.* Whitepaper. 6.12.2017. CRASHOVERRIDE: Analysing the Malware that Attacks Power Grids | Dragos (access 23.03.2021).

24. ePUAP (2021) ePUAP - Strefa klienta (access 23/07/2021).

25. *Europe* (1994) *and the global information society. Recommendations of the high-level group on the information society to the Corfu European Council (Bangeman group).* In: European Commission: *Growth* competitiveness *and employment. White paper follow-up Report on Europe and the global information society. Interim report on trans-European networks. Progress report on employment. Extracts of the conclusions of the Presidency of the Corfu European Council.* In: *Bulletin of the European Union,* Supplement 2/94. Luxembourg: Office for Official Publications of the European Communities, 135 s. info_society_bangeman_report.pdf (pitt.edu) (access 14.07.2021).

26. *Europe* (2020) 2020. *A strategy for smart, sustainable and inclusive growth* COM/2010/2020 final.

27. European (2020) *Commission*: *Shaping Europe's digital future. I-DESI-2020. How digital is Europe compared to other major world economies?* I-DESI 2020: How digital is Europe compared to other major world economies? | Shaping Europe's digital future (europa.eu) (access 24.07.2021).

28. European (2020) Union Agency for Cybersecurity, *Cybersecurity Certification. EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS,* p. 281 ENISA_candidate scheme_EUCC (4).pdf (access 23.07./2021).

29. European (2021) Commission: *Shaping Europe's digital future. Digital Europe programme: A proposed 7.5 billion of funding for 2021-2027. Factsheet/ Infographic.* 8 March 2021. Digital Europe Programme: A proposed €7.5 billion of funding for 2021-2027 | Shaping Europe's digital future (europa.eu) (access 23.04.2021).

30. European (2021) *Commission*: *Shaping Europe's digital future. Quantum Technologies Flagship.* 9 March 2021. Quantum Technologies Flagship | Shaping Europe's digital future (europa.eu) (access 20.07.2021).

31. European (2021) Council, Council of the European Union: *Long-term UE budget 2021-2021 and recovery package,* 1 January 2021. Long-term EU budget 2021-2027 and recovery package - Consilium (europa.eu) (access 21.03.2021).

32. European (2021) Union Agency for Cybersecurity. *EU cybersecurity certification framework.* Certification — ENISA (europa.eu) (access 23.07.2021).

33. European (2021) Union Agency for Cybersecurity. *Securing EU's Vision on 5G; Cybersecurity Certification.* Press release 3 February 2021 Securing EU's Vision on 5G: Cybersecurity Certification — ENISA (europa.eu) (access 20.03.2021).

34. Europol (2021) European Cybercrime Centre – EC3 European Cybercrime Centre - EC3 | About Europol | Europol (europa.eu) (access 24.07.2021).
35. FIRST (2021) – the Forum of Incident Response and Security Teams. About FIRST (access 02.07.2021).
36. Fournaris (2019) A.P, Lampropoulos K., Tordera E.M. (eds.) *Information and Operational Technology Security Systems. First International Workshop IOSec 2018 CIPSEC Project* , Heraklion, Creta, Greece, 13 September 2018. Revised selected papers. [eBook]. Cham (Switzerland). Springer Nature, 2019, 147 pp.
37. Furnkramz (2020) G.. *The Quantum Internet. Ultrafast and Safe from Hackers*. [e-Book] Cham (Switzerland) Springer Nature, 2020, 269 p..
38. Furusawa (2011) A., Peter van Loock: *Quantum Teleportation and Entanglement. A Hybrid Approach to Optical Quantum Information Processing*. [e.Book]. Weiheim (Germany): Wiley-VCH Verlag GmbH & Co. 2011, 341 p..
39. GOV.UK (2020) *Huawei to be removed from UK 5G networks by 2027*. Press release 14 July 2020. Huawei to be removed from UK 5G networks by 2027 - GOV.UK (www.gov.uk) (access 21.07.2021).
40. Grabowska (2020) M., *Europejskie społeczeństwo gigabitowe* [*European Gigabit Society*] In: *Studia Europejskie – Studies in European Affairs*, 2020, no. 1, p. 151-172..
41. *Green* (1997) *Paper on the Convergence of the telecommunications, media and information technology. Towards an Information Society Approach.* COM (97)632 final, 3 December 1997, p. 38.
42. *Growth*, (1993) *competitiveness, employment. The challenges and ways forward into the 21st century. White papers.* COM (93)700, 3 December 1993 Part A and B.
43. Hartman (2019) Leigh, *Countries agree on 5G security in Prague*, 13 May 2019. Countries agree on 5G security in Prague | ShareAmerica (access 23.04.2021).
44. Hodges (2014) A., *Alan Turing: Enigma* (translation from English by W. Bartol). Warsaw: Publishing House: Albatros Andrzej Kuryłowicz S.C., 715 pp.
45. International (2019) Telecommunication Union (ITU) *Global Cybersecurity Index 2018. ITU Publications. Studies and Research*. Switzerland, Geneva, 2019, 87 p. Global Cybersecurity Index 2018 ${field:Subtitle report} (itu.int) (access 23.04.2021).

46. Kitagawa (2021) F., *From Technopolis, cluster to regional science policy?: Japanese regional development policy 1980s-2020s. The history of Japanese regional development policy and its assessment*. In: Academia.edu (PDF) From Technopolis, Cluster to Regional Science policy?: Japanese Regional Development Policy 1980s-2000s | Fumi Kitagawa - Academia.edu (access 24.07.2021).

47. *Lisbon* (2000) *European Council 23 and 24 March 2000. Presidency Conclusions* Lisbon European Council 23-24.03.2000: Conclusions of the Presidency (europa.eu) (access 24.04.2021).

48. Ministry (2019) of Digital Affairs *Cybersecurity Strategy of the Republic of Poland for 2019-2024* Strategia_Cyberbezpieczeństwa_RP_w_języku_angielskim (4).pdf (access 02.07.2021).

49. NASK (2019) *Security Landscape of the Polish Internet CERT Polska 2019 Annual Report.* NASK PIB/CERT, Poland, 146 p. (co-financed by EU instrument Connecting Europe Facility) https://www.cert.pl/uploads/docs/Raport_CP_2019.pdf (access 23.04.2021).

50. NASK (2021) CERT-PL CERT Polska (access 02.07.2021).

51. National (2021) Bank of Poland. The National Certification Centre (NCCert) Narodowe Centrum Certyfikacji (nccert.pl) (access 24.07.2021).

52. *Network* (2001) *and Information Security: Proposal for A European Policy Approach*. COM (2001) 298 COM(2001)298 - Network and Information Security: Proposal for A European Policy Approach - EU monitor (access 24.07.2021).

53. Nora (1978), S., Minc, A. *L'informatisation de la societe: rapport a M. le President de la Republique*. Paris: La Documentation Francaise, Janvier, [900 pp.]

54. Park (2021) S., Specter M., Narula N., Rivesr R.L. *Going from bad to worse: from Internet voting to blockchain voting*. In: *Journal of Cybersecurity* 2021 vol. 7 issue 1. Going from bad to worse: from Internet voting to blockchain voting | Journal of Cybersecurity | Oxford Academic (oup.com) (access 23.07.2021).

55. *Presidency* (2001) *Conclusions Gōteborg. European Council 15 and 16 June 2001,* p. 22 00200-r1en1.pdf (europa.eu) (access 26.07.2001).

56. *Regulation* (2004) *(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 L 77, 13.3.2004, pp. 1–11.

57. *Regulation* (2014) (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 L 257, 28.8.2014, p. 73-114.
58. *Regulation* (2016) *(EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).* OJ L 119, 4.5.2016, p. 1–88.
59. *Regulation* (2019) *(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) PE/86/2018/REV/1*. OJ L 151, 7.6.2019, pp. 15–69.
60. Rejewski (1980) M., *An Application of the Theory of Permutations in Breaking the Enigma Cipher*. In: *Applicationes Mathematicae* 16 (4) January, p. 543-559
61. Rejewski (1981) M., How *Polish mathematicians deciphered the Enigma*. In: *Annals of the History of Computing*, 3. p. 213-234
62. *Resolution (1994) on the recommendation to the European Council: "Europe and the global information society" and the Communication from the Commission to the Council and the European Parliament and to the Economic and Social Committee and the Committee of the Regions: "Europe's way to the information society: an action plan'*. OJ C 363 19.12.1994, p. 33.
63. *Single* (1987) European *Act*, OJ L 169, 29.6.1987, p. 1-28 (Title VI).
64. *Treaty* (1992) *on European Union*. OJ C 191, 29.7.1992, p.1-112 (Title XIII)
65. *Uchwała (2019) nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2019-2024.* M.P..2019 r. poz. 1037
66. *Ustawa* (2018) z *dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.* Dz. U. 2018 poz.1560.