Anna Molnár

European Union – Cybersecurity

Introduction

It is a commonplace to state that European societies, governmental and private sectors are increasingly dependent on digital technologies. Electronic networks and information systems have developed to be part of our daily lives. In recent years, digital technology has become an essential tool on which not only all sectors of the economy, but also every area of our lives rely. Highlighting only a few of them, such as electricity or transport networks, production and financial processes, and health care systems, a significant degree of interdependence and interconnection can be observed.

As a result, the European economies, governmental or defence infrastructures, and in this context, even the functioning of democracy, European values and liberties can be threatened by malicious cyber activities. Europe's security largely depends on the cyber resilience of Member States and EU institutions: the ability to prepare for and to respond to the ever-changing and growing intensity of cyber threats. Today, many business models rely on the smooth operation of the Internet and information systems. In parallel, the economic impact of cybercrime is steadily increasing. In addition to racketeering, many other threats are a major challenge for European economic and political actors. In today's computer age, the protection of personal data also plays a crucial role in the implementation of cybersecurity.

The widely used term of cybersecurity is not limited to network and information security in the policy circles of the EU. According to a report prepared by the European Court of Auditors, the cybersecurity ecosystem includes any illegal activity realised by the use of digital technologies in cyberspace. It refers to cybercrimes like computer virus attacks and non-cash payment fraud, and the dissemination of online child sexual abuse material. It includes disinformation campaigns to influence online debate and suspected electoral interference. According to the definition of Europol, a connection between cybercrime and

https://doi.org/10.36250/01039_02

terrorism can be observed.[1] Not only government institutions, but also European Internet users and companies have experienced several cybersecurity incidents. It is crucial to guarantee that devices and networks are protected to deter cyber-attacks. Despite the fact that the European Union has started to strengthen its comprehensive cybersecurity governance, an analysis prepared by the European Court of Auditors has highlighted several weaknesses and shortfalls in the governance and in the legislative framework in 2019. The complex ecosystem of the EU's cybersecurity policy is closely linked to internal policy areas; regarding internal policy areas, it covers justice and home affairs, the digital single market and research policies as well. The EU has become increasingly active in external policy areas as well, and cybersecurity is closely linked to diplomacy, and to security and defence policy.[2]

The Strategic Framework and Regulations of the European Union

The Strategic Framework since 2000

The EU has been an observer organisation to the Cybercrime Convention Committee of the Council of Europe since 2001 (the Budapest Convention), which provided a framework for the promotion of international cooperation and legislation against cybercrime. Despite the growing awareness, the threats and challenges related to cybersecurity were only briefly mentioned by the strategies of the EU during the first decade of the 21st century. In 2003, the European Security Strategy already implicitly referred to cybersecurity. The document developed by Javier Solana, High Representative for the Common Foreign and Security Policy, only highlighted the danger of terrorist movements connected by electronic networks.[3] In 2005, the European Commission published a comprehensive strategy entitled *i2010: A European Information Society for Growth and Employment.* The new strategy aimed to promote the development of an open and competitive digital economy and emphasised the key role of ICT (information and communication

[1] European Court of Auditors (2019): Challenges to Effective EU Cybersecurity Policy. *Briefing Paper,* March 2019. 6.

[2] European Court of Auditors (2019): op. cit. 12.

[3] Council of the European Union: *European Security Strategy. A Secure Europe in a Better World.* Brussels, General Secretariat of the Council, 2009. 30.

technology) in social inclusion and quality of life. The document mentions the issue of security in many cases. In the interest of a secure and reliable ICT, the European Commission articulated the need to develop a Strategy for a Secure Information Society.[4]

Additionally, the 2008 review of the European Security Strategy has already addressed the basic issues of cybersecurity in a short section. The document emphasised that modern economies are highly dependent on critical infrastructure such as the Internet. Internet-based crime was mentioned in the Strategy for a Secure European Information Society, adopted in 2006. However, as a result of attacks on governments of Member States or private IT systems, a new dimension related to a potential new economic, political and military weapon was added. The document underlined the need for more work to explore a comprehensive EU approach, raise awareness and enhance international cooperation.[5] The Internal Security Strategy of the European Union, adopted in 2010, drew attention to the dangers of cybercrime in the Union.[6]

In May 2010, after the Lisbon Strategy, the European Commission launched the *Europe 2020 Strategy,* which aimed at reducing vulnerability and increasing competitiveness.[7] As one of the flagship initiatives of the new strategy, the European Commission has launched the *Digital Agenda for Europe (DAE).* The agenda aimed to make the use of information and communication technologies (ICT) a key factor in achieving the goals set in the *Europe 2020 Strategy.* The European Commission has built the *Digital Single Market Strategy* on three pillars to ensure a fair, open and secure digital environment: (1) Ensuring better access to digital goods and services for consumers and businesses across Europe; (2) Creating the right conditions for digital networks and services; and (3) Maximising the growth potential of the digital economy.[8]

[4] European Commission: Brussels, 1.6.2005, COM(2005) 229 final, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions "i2010 – A European Information Society for Growth and Employment". Commission of the European Communities, 2005.

[5] Council of the European Union: *Report on the Implementation of the European Security Strategy. Providing Security in a Changing World.* Brussels, 11 December 2008. 5.

[6] Council of the European Union: *Internal Security Strategy for the European Union. Towards a European Security Model.* Brussels, General Secretariat of the Council, 2010. 7.

[7] László Kovács: *Kiberbiztonság és stratégia.* Budapest, Dialóg Campus, 2018. 85.

[8] European Commission: *Shaping the Digital Single Market.* 2020.

In particular, the EU intended to respond adequately to challenges in the digital domain, such as the fragmentation of the digital market, interoperability issues, the very rapid spread of cybercrime, the low level of R&D and investment in it, or the low level of digital literacy in many regions of the EU.[9]

Table 1. *Strategy Papers of the European Union on Cybersecurity*

Year	Strategy Papers of the European Union
2003	European Security Strategy
2005	i2010: European Information Society for Growth and Employment
2006	Strategy for a Secure European Information Society
2008	Report on the Implementation of the European Security Strategy. Providing Security in a Changing World
2010	Internal Security Strategy for the European Union. Towards a European Security Model
2010	A Digital Agenda for Europe
2013	Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
2014	EU Cyber Defence Policy Framework
2015	Council Conclusions on Cyber Diplomacy
2015	Digital Single Market Strategy for Europe
2016	Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy
2017	Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU
2018	EU Cyber Defence Policy Framework
2020	The EU's Cybersecurity Strategy for the Digital Decade
2021–2027	Digital Europe Programme (DIGITAL)

Source: Compiled by the author based on Rehrl (2018): op. cit. 26.

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013)

The EU began developing its first comprehensive cybersecurity strategy in 2012–2013. All of this happened at a time when developed countries were realising the strategic importance of cybersecurity challenges. Compared to NATO, whose

[9] Kovács (2018): op. cit. 86.

first strategies (2008, 2011) focused solely on protecting its own IT network, the first EU strategy covered almost all areas of EU competences.[10]

Following the entry into force of the Lisbon Treaty, the European External Action Service and the European Commission, under the leadership of EU High Representative for Foreign Affairs and Security Policy Catherine Ashton, also worked together to draft the joint communication. In 2013 the *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* was adopted by the European External Action Service and the European Commission. This document first mentioned the need for a coherent EU international cyberspace policy and cyber defence objectives. One of the main goals and principles of the strategy was to uphold EU core values and promote a peaceful, open and transparent use of cyber technologies.[11]

The implementation of the strategy was primarily the responsibility of some Directorates-General of the European Commission. The Directorate-General for Content, Technology and Communication Networks (DG CNETC) was responsible for legislation, industrial policy and research and development in the new cyber areas. The Directorate-General for Migration and EU Home Affairs (DG HOME) has been responsible for shaping cyber law enforcement policy and promoting cooperation between Member States in this area.

The principles set out in the strategy were in line with the general principles and values of the EU: (1) The core values of the European Union apply to the digital world as much as to the physical world; (2) Protection of fundamental rights, freedom of expression, personal data and privacy; (3) Access for all; (4) Democratic and efficient multi-stakeholder governance; (5) Shared responsibility to ensure security.

However, the strategy sets out five priorities: (1) Achieving resilience to cyberattacks; (2) A drastic reduction in cybercrime; (3) Developing cyber defence policy and capabilities for the Common Security and Defence Policy (CSDP); (4) Development of cybersecurity industry and technological resources; (5) Establishing a coherent international policy on cyberspace for the European Union and promoting the Union's core values.[12]

[10] Jochen Rehrl (ed.): *Handbook on Cybersecurity. The Common Security and Defence Policy of the European Union.* Luxembourg Publications Office of the European Union, 2018. 18.

[11] European Commission: *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* JOIN/2013/01 final.

[12] Ibid.

EU Cyber Defence Policy Framework (2014)

The European External Action Service (EEAS) is responsible for promoting cyber defence activities and developing international cyber policy goals including cyber diplomacy and strategic communication, and hosts intelligence and analysis centres.[13] According to the European Council Conclusions on CSDP in December 2013, the cyber defence policy framework was developed by the EEAS together with the European Commission and the European Defence Agency.[14] Under the leadership of the EEAS, the EU Cyber Defence Policy Framework was completed in 2014.

The document established the following objectives:

1. Supporting the development of cyber defence capabilities of Member States in areas related to the common security and defence policy
2. Enhancing the protection of communication and information networks used by the EEAS in the field of CSDP
3. Promoting civil–military cooperation and synergies with the wider EU cyber policies to address the new challenges
4. Help cooperation with the private sector on cyber defence capability development
5. Improving training, education and exercise opportunities
6. Enhancing cooperation with relevant international partners, in particular with NATO[15]

Directive on the Security of Network and Information Systems (2016)

The European Union adopted the first EU-wide legislation on cybersecurity in 2016 with the Directive (EU) 2016/1148 of the European Parliament and the Council on the security of network and information systems (NIS). The NIS Directive had to be transposed into national laws of the EU Member States

[13] European Court of Auditors (2019): op. cit. 10.

[14] European Council: *European Council Conclusions 19/21 December 2013.*

[15] Council of the European Union: *EU Cyber Defence Policy Framework.* Brussels, 18 November 2014.

by 9 May 2018 and the units providing essential services had to be identified by 9 November 2018.

The aim of the NIS Directive is to introduce comprehensive measures that can increase the level of security of network and information systems and services which play a vital role in the economy and society of the Union. Implementing the directive will enable EU countries to prepare for and respond to cyberattacks. To this end, it has become necessary at Member State level to (1) designate competent authorities; (2) set up Computer Security Incident Response teams (CSIRTs); and (3) adopt national cybersecurity strategies. The measures introduced will strengthen cooperation at both strategic and technical levels in the European Union.[16]

However, the Directive obliges essential and digital service providers (such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructures) to take appropriate security measures and to inform the relevant national authorities of serious incidents.

Under the new rules, EU Member States must also adopt national cybersecurity strategies for network and information systems. Strategies at the national level should include the following issues:

> "(a) the objectives and priorities of the national strategy on the security of network and information systems;
> (b) a governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors;
> (c) the identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors;
> (d) an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems;
> (e) an indication of the research and development plans relating to the national strategy on the security of network and information systems;
> (f) a risk assessment plan to identify risks;
> (g) a list of the various actors involved in the implementation of the national strategy on the security of network and information systems.
>
> It is the responsibility of the national competent authorities to monitor the application of the Directive. To this end, national authorities should assess the level of security of network and information systems. They should also participate in the work of the Cooperation

[16] 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.

> Group, which is composed of representatives of the Member States, the Commission and European Commission and the European Network and Information Security Agency (ENISA). The national competent authorities shall inform the public about individual incidents where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident."[17]

Global Strategy (2016)

The European Union's Global Strategy for Foreign and Security Policy (hereinafter referred to as the Global Strategy), adopted in 2016, has already addressed the issue of cybersecurity in details. The strategy calls for the strengthening of the EU as a security community and the development of capabilities for the protection of EU citizens and the response to external crises. In addition, the interoperability of civilian and military capabilities needs to be strengthened.

The Global Strategy emphasises that the Union will focus on cybersecurity in the future and will be able to respond more effectively to cyber threats. With this new strategy, the EU intended to address open, free and secure cyberspace in all policy areas.[18]

> "The EU will increase its focus on cyber security, equipping the EU and assisting Member States in protecting themselves against cyber threats while maintaining an open, free and safe cyberspace. This entails strengthening the technological capabilities aimed at mitigating threats and the resilience of critical infrastructure, networks and services, and reducing cybercrime. It means fostering innovative information and communication technology (ICT) systems which guarantee the availability and integrity of data, while ensuring security within the European digital space through appropriate policies on the location of data storage and the certification of digital products and services. It requires weaving cyber issues across all policy areas, reinforcing the cyber elements in CSDP missions and operations, and further developing platforms for cooperation. The EU will support political, operational and technical cyber cooperation between Member States, notably on analysis and consequence management, and foster shared assessments between EU structures and the relevant institutions in Member States. It will enhance its cyber security cooperation with core partners such as the US and NATO. The EU's response will also be embedded in strong public-private partnerships. Cooperation and information-sharing between Member States, institutions, the private sector and civil society can foster a common cyber security culture, and raise preparedness for possible cyber disruptions and attacks."[19]

[17] Directive (EU) 2016/1148.

[18] European External Action Service: *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy.* 2016.

[19] Ibid. 21–22.

Review of the Cyber Security Strategy (2017)

As the goals set in the 2013 cybersecurity strategy were not always met and changes in cybersecurity threats have taken place to such an extent in recent years, it has become inevitable to review the first strategy and develop a new one. Disruptive computer operations against critical infrastructures, democratic institutions and the Internet of Things (IoT), as well as large-scale botnet attacks and global ransomware infections such as "WannaCry" and "NotPetya") drew attention to cyber risks and the need for proactive action at EU level.[20]

Under the leadership of the European Commission, the revision of the EU cybersecurity strategy was completed in 2017. The joint communication from the EC and the High Representative for Foreign Affairs and Security Policy to the European Parliament and the Council was entitled *Resilience, Deterrence, Defence: Building Strong Cybersecurity for the EU.*[21]

The strategy highlights as follows:

> "Cybersecurity is critical to both our prosperity and our security. As our daily lives and economies become increasingly dependent on digital technologies, we become more and more exposed. Cybersecurity incidents are diversifying both in terms of who is responsible and what they seek to achieve. Malicious cyber activities not only threaten our economies and the drive to the Digital Single Market, but also the very functioning of our democracies, our freedoms and our values. Our future security depends on transforming our ability to protect the EU against cyber threats: both civilian infrastructure and military capacity rely on secure digital systems. This has been recognised by the June 2017 European Council, as well as in the Global Strategy on Foreign and Security Policy for the European Union."[22]

The document underlines that:

> "While Member States remain responsible for national security, the scale and cross-border nature of the threat make a powerful case for EU action providing incentives and support for Member States to develop and maintain more and better national cybersecurity capabilities, while at the same time building EU-level capacity."[23]

[20] Rehrl (2018): op. cit. 23.

[21] European Commission: *Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU.* Brussels, 13.9.2017, JOIN(2017) 450 final.

[22] Ibid.

[23] Ibid.

The new strategy proposed new measures to ensure the EU's resilience, deterrence and protection against cyberattacks. These proposals included the strengthening of the European Network and Information Security Agency (ENISA), the development of a voluntary EU cybersecurity certification framework to enhance the cybersecurity of digital products and services, and a plan for rapid, coordinated response to large-scale cybersecurity incidents and crises. The Commission proposed a permanent mandate for the ENISA, which, having a strong advisory role on policy development and implementation, will support Member States, EU institutions and businesses in key areas. The joint communication highlights cyber defence as a priority for EU actions. According to the document, the 2014 EU cyber defence policy framework needed to be renewed.[24]

The 2017 Cybersecurity Package and the Digital Single Market Strategy

In September 2017, in his annual speech at the European Parliament (State of the Union), President Jean-Claude Juncker highlighted the importance of the progress during the previous three years in keeping Europeans safe online. But he also stated that Europe was not well prepared against cyberattacks. Jean-Claude Juncker argued strongly in favour of establishing new tools against cyberattacks, such as the European Cybersecurity Agency. The European Commission and the High Representative proposed a Cybersecurity Package, a wide-ranging set of measures to strengthen cybersecurity in the EU. This included a proposal for an EU Cybersecurity Agency, a new EU-wide certification framework for products and services in the digital world, organisation of yearly pan-European cybersecurity exercises. According to Federica Mogherini, High Representative of the Union, the EU is developing an international cyber policy supporting an open, free and secure cyberspace. It also promotes all efforts in order to establish "norms of responsible state behaviour, apply international law and confidence building measures in cybersecurity".[25]

[24] Ibid.

[25] European Commission: *State of the Union 2017 – Cybersecurity: Commission Scales Up EU's Response to Cyber-attacks.* Brussels, 19 September 2017.

Cybersecurity Act

As part of the cybersecurity package adopted in September 2017, the realisation of a new legislation on cybersecurity (known as the Cybersecurity Act), which is one of the priorities of the Digital Single Market Strategy, has begun. In September 2018, the European Commission proposed the establishment of a European Cybersecurity Industrial, Technology and Research Competence Centre and a network of cybersecurity competence centres.[26]

The priority of the Digital Single Market Strategy (2015) was to remove barriers to online transactions and provide consumers with secure access to products and services.[27] The new European Cybersecurity Act was proposed in 2017 and was adopted in 2019 by the European Parliament and the Council. The new legislation covered the following areas: setting the new mandate of ENISA, the EU Agency for Cybersecurity and establishing the European cybersecurity certification framework. ENISA will support Member States in effective response to cyberattacks in the new cybersecurity certification framework. With the entry into force of the Cybersecurity Act, the ENISA, the EU Agency for Cybersecurity will have a permanent mandate, strengthened responsibilities and increased resources.[28]

Cyber Defence and Permanent Structured Cooperation (PESCO)

From 2017, the process of implementing the permanent structured cooperation (PESCO) provided by the Lisbon Treaty began with the participation of 25 Member States. The participating Countries have committed themselves to stepping up their efforts in the field of cyber defence, as well. Since 2017, 6 cyber-related PESCO projects have been launched:

1. European Secure Software Defined Radio (ESSOR)
2. Cyber Threats and Incident Response Information Sharing Platform

[26] European Commission: *Shaping Europe's Digital Future. Policy, European Cybersecurity Industrial, Technology and Research Competence Centre.* Brussels, 19 September 2018.

[27] European Commission: *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe.* Brussels, 6.5.2015, COM(2015) 192 final.

[28] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA.

3. Cyber Rapid Response Teams and Mutual Assistance in Cyber Security
4. Strategic Command and Control (C2) Systems for CSDP Missions and Operations
5. European High Atmosphere Airship Platform (EHAAP) – Persistent Intelligence, Surveillance and Reconnaissance (ISR) Capability
6. One Deployable Special Operations Forces (SOF) Tactical Command and Control (C2) Command Post (CP) for Small Joint Operations (SJO) – (SOCC) for SJO[29]

European Union Cyber Defence Policy Framework (2018)

In October 2018, the European Council called for measures able to respond to and deter cyberattacks and to build strong cybersecurity in the EU in order to strengthen its capacities. In view of the changing security challenges, the Council adopted a revised version of the EU Cyber Defence Policy Framework in October 2018. The updated version of the framework identified priority areas for cyber defence and clarified the roles of actors.

Scope and Objectives

> "To respond to changing security challenges, the EU and its Member States have to strengthen cyber resilience and to develop robust cyber security and defence capabilities. The EU Cyber Defence Policy Framework (CDPF) supports the development of cyber defence capabilities of EU Member States as well as the strengthening of the cyber protection of the EU security and defence infrastructure, without prejudice to national legislation of Member States and EU legislation, including, when it is defined, the scope of cyber defence.
> Cyberspace is the fifth domain of operations, alongside the domains of land, sea, air, and space: the successful implementation of EU missions and operations is increasingly dependent on uninterrupted access to a secure cyberspace, and thus requires robust and resilient cyber operational capabilities.
> The objective of the updated CDPF is to further develop EU cyber defence policy by taking into account relevant developments in other relevant fora and policy areas and the implementation of the CDPF since 2014. The CDPF identifies priority areas for cyber defence and clarifies the roles of the different European actors, whilst fully respecting the responsibilities and competences of Union actors and the Member States as well as the institutional framework of the EU and its decision-making autonomy."[30]

[29] EU Cyber Direct: *Cyber-related PESCO Projects.* Brussels, 12 November 2019; Council of the European Union: *Permanent Structured Cooperation (PESCO)'s Projects – Overview.* 2019.

[30] Council of the European Union: *EU Cyber Defence Policy Framework, (as updated in 2018).* Brussels, 19 November 2018(OR. en).

The document refers to the implementation of the goals and priorities set in the 2016 Global Strategy and the Joint Declaration on EU–NATO Cooperation. However, it emphasised that a number of other EU policies also contribute to achieving the objectives of cyber defence policy. This policy framework also takes into account regulations in civil areas (e.g. the Network and Information Security Directive) in order to contribute to the EU's strategic autonomy also in the area of cyberspace.

The policy framework highlights that, in accordance with the Council Conclusions on Cybersecurity of November 2017, there are growing linkages between the areas of cybersecurity and defence, and that there is a need to encourage cooperation between civilian and military incident response communities. The Council document emphasised that in a particularly serious cyber incident or crisis, the Solidarity Clause and/or the Mutual Assistance Clause of the Lisbon Treaty could also be activated.[31]

The policy framework identifies six priority areas: (1) developing cyber defence capabilities; (2) protecting EU CSDP communication and information networks; (3) training and exercises; (4) research and technology; (5) civil–military cooperation; and (6) enhancing cooperation with international partners.[32]

The EU's Cybersecurity Strategy for the Digital Decade (2020)

In December 2020, the new EU's cybersecurity strategy was completed by the European Commission and the European External Action Service. The deep crises caused by the Covid-19 pandemic not only accelerated the process of digitalisation but also led to a higher level of awareness in the EU. The strategy aims to strengthen resilience to cyber threats and provide reliable and secure services and digital tools for all citizens and businesses. The document aims to enable citizens and businesses to acquire these benefits. The strategy underlines the crucial role of cybersecurity for a growing economy, democracy and society. The objective of this strategy is to reinforce user confidence in digital tools. The strategy emphasises three main areas of EU action: (1) resilience, technological sovereignty and leadership; (2) building operational capacity to prevent, deter and respond (to cyberattacks); and (3) advancing a global and open cyberspace through increased cooperation.[33]

[31] Ibid. 6.

[32] Ibid. 8.

[33] European Commission: *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 16.12.2020 JOIN(2020) 18 final.

In March 2021, the Council adopted conclusions on the cybersecurity strategy, highlighting that cybersecurity is an essential tool for building a resilient, green and digital Europe. The Council sets as a key objective of realising strategic autonomy at the same time as preserving an open economy. The conclusions aim at enabling the EU to make autonomous choices in the field of cybersecurity and to achieve the EU's digital leadership and strategic capacities.[34]

Digital Europe Programme (DIGITAL) (2021–2027)

The Digital Europe Programme (DIGITAL) is a part of the current long-term EU budget, the Multiannual Financial Framework 2021–2027. It is a new funding programme to bring digital technologies to businesses, citizens and public administrations. It provides strategic funding with a budget of €7.5 billion to support projects in five key capacity areas: (1) in supercomputing; (2) artificial intelligence; (3) cybersecurity; (4) advanced digital skills; and (5) ensuring a wide use of digital technologies across the economy and society, including through Digital Innovation Hubs. The new EU funding program aims to speed up the economic recovery and shape the digital transformation of Europe's society and economy, providing benefits to a wide range of stakeholders, but especially to small and medium-sized enterprises.[35]

The Institutional Framework Regarding the Cybersecurity of the EU

Due to the comprehensive nature of this issue, practically all institutions, bodies and agencies in the European Union are involved in the preparation and implementation of cybersecurity policy.

[34] Council of the European Union: *Draft Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 9 March 2021(OR. en).

[35] European Commission: *The Digital Europe Programme.* s. a.; Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 Establishing the Digital Europe Programme and Repealing Decision (EU) 2015/2240 (Text with EEA Relevance).

Table 2. *Cybersecurity in the EU: Areas of responsibility and institutional framework*

Cybersecurity			
Single market	**Freedom, security and justice**	**CFSP: Cyber diplomacy**	**CSDP: Cyber defence**
European Commission DGs		EEAS	
CERT-EU	Europol (EC3)	SIAC (EU INTCEN, Hybrid Fusion Cell, EUMS INT)	
ENISA	Eurojust	EU SITROOM	
CSIRT network			
	EU-LISA	ESDC	
ECCC			EDA
			GSA

Source: Compiled by the author based on Bendiek (2018): op. cit. 4.

European Commission

The European Commission intends to strengthen cybersecurity capabilities. It also initiates and promotes policy-making and legislative processes in this field. The main Directorates-General (DG) responsible for areas related to cybersecurity are DG Connect (Communications Networks, Content and Technology) and DG Migration and Home (cybercrime). The main tasks of the Directorate-General Connect are linked to developing a digital single market and promoting policy-making processes related to cybersecurity. The Directorate-General Migration and Home is responsible for initiating and developing cybercrime policy. The Directorate-General for Informatics (DG Digit) provides digital services for departments of the European Commission and other EU institutions. Digit hosts CERT-EU (Computer Emergency Response Team).[36] DG Human Resources and Security is responsible for the Commission's staff, information and assets. It also provides investigations regarding incidents that covers counter-intelligence and counter-terrorism activities as well.[37]

[36] European Court of Auditors (2019): op. cit. 31.

[37] European Commission: *Departments and Executive Agencies.* s. a.

Computer Emergency Response Team (CERT-EU)

In the Digital Agenda for Europe adopted in 2010, the European Commission decided to establish a Computer Emergency Response Team for the EU institutions (CERT-EU) supporting all Union institutions, bodies and agencies. According to the Agenda, these CERTs had to be set up not only at EU level but also at Member State level in order to have a network of national and governmental CERTs in place by 2012. The CERT-EU was established in 2011 and it is hosted by the European Commission. Following a one-year pilot phase, the CERTs have been operating at full capacity since September 2012. The CERT-EU is composed of IT security experts from the main EU Institutions, and it cooperates with other CERTs in the Members States and with specialised IT security companies. The task of the newly set up permanent groups is to help them to respond to incidents, particularly those affecting information security. CERT-EU prepares reports and briefings on cyber threats concerning EU institutions, bodies and agencies. It provides an information-sharing platform. In 2018, CERT-EU finalised a non-binding memorandum of understanding with ENISA, EC3 and the European Defence Agency in order to increase cooperation and coordination with those agencies. It also signed a technical agreement with NATO's computer incident response capability (NCIRC).[38]

The role of CERTs is to prevent weaknesses in network security, to identify threats and to address vulnerabilities. In order to maintain and restore system security, the groups warn their clients about existing security vulnerabilities and threats, propose measures to reduce the risks.

European Network and Information Security Agency (ENISA)

The European Network and Information Security Agency (ENISA) was established in 2004. The agency, which has a mainly advisory role, has been operating in Athens and has had a second office in Heraklion since 2005. From 2005, the Agency's role was to

[38] European Court of Auditors (2019): op. cit. 6.

> "contribute to securing Europe's information society by raising awareness of network and information security and to develop and promote a culture of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organizations in the Union."[39]

In parallel with the development of the first cybersecurity strategy, a new Regulation of the European Parliament and of the Council on the operation of ENISA was adopted on 21 May 2013, extending the Agency's mandate until 2020 and strengthening its capacity to tackle cyberattacks and other information security challenges.[40]

The first EU legislation on cybersecurity, the 2016 NIS Directive gave a central role to the ENISA in supporting the implementation of the Directive. The Agency provides the secretariat for the Network Security Response Teams (CSIRTs) and actively supports cooperation between CSIRTs.

Since 2019, following the new legislation of the Cybersecurity Act (Regulation 2019/881), ENISA has been tasked to support Member States, EU institutions and all other stakeholders in their cyber policies, and to prepare the 'European cybersecurity certification schemes' that serve as the basis for certification of ICT products, processes and services that support the proper delivery of the Digital Single Market. ENISA will play a central role in the development of certification schemes.

The Agency's new tasks will include:

- organising pan-European Cybersecurity Exercises
- the development and evaluation of National Cybersecurity Strategies
- CSIRTs cooperation and capacity building
- studies on IoT and smart infrastructures, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, identifying the cyber threat landscape, and others
- supporting the development and implementation of the European Union's policy and law on matters relating to network and information security (NIS)
- assisting Member States and European Union institutions, bodies and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis[41]

[39] 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), Article 1(1).

[40] Regulation (EU) No 526/2013.

[41] ENISA: *About ENISA – The European Union Agency for Cybersecurity.* s. a.

The exercises organised by ENISA have helped to prepare national authorities to strengthen preparedness and resilience to cyber threats.

Computer Security Incident Response Team (CSIRTs)

The transposition of the 2016 Directive of the European Parliament and of the Council on the security of network and information systems (2016/1148) at Member State level necessitated the establishment of a network of Computer Security Incident Response Teams, i.e. CSIRTs. The EU-wide network is composed of CSIRTs in the Member States and representatives of the Network Security Emergency Response Teams (CERT-EU). The European Commission takes part in the network as an observer. ENISA supports the cooperation between CSIRTs appointed by the EU Member States, and it provides the secretariat. The CSIRTs Network offers a forum to exchange information and build trust.[42]

European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC)

In April 2021, the Council reinforced the selection of Bucharest as the seat of the new European Cybersecurity Industrial, Technology and Research Competence Centre (Cybersecurity Competence Centre, ECCC), which will improve the coordination of research and innovation in cybersecurity. It will also bring together the main European stakeholders, and it will help to promote pooling investment in cybersecurity research, technology and industrial development. The new centre will closely cooperate with ENISA.[43]

In May 2021, the European Parliament and the Council adopted the regulation establishing the ECCC and the Network of National Coordination Centres (Cyber NCCs).[44] Although the ECCC is not a formal EU agency, but

[42] ENISA: *CSIRTs Network*. s. a.

[43] Council of the European Union: *Draft Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 9 March 2021(OR. en).

[44] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 Establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

> "it will pool resources from the EU, Member States and industry to improve and strengthen technological and industrial cybersecurity capacities, enhancing the EU's strategic autonomy in the field of cybersecurity. It will offer a possibility to consolidate part of the cybersecurity-related activities funded under Horizon Europe, the Digital Europe Programme and the Recovery and Resilience Facility – funding streams totalling up to EUR 4.5 billion over the next six years."[45]

The aim of this process is to create an EU Cyber Shield composed of a network of Security Operations Centres by 2023, in order to detect cyberattacks early enough to enable proactive actions. In the future, it may be able to use Artificial Intelligence-powered technologies. Numerous Member States have planned the development of such national centres in the framework of their Recovery and Resilience plans. The European Commission allocates funds from the Digital Europe Programme to support their efforts.[46]

Europol EC3

In 2013, the European Cybercrime Centre (EC3) was set up at the headquarters of Europol in The Hague. The aim of the new centre was to protect European citizens and businesses from cyber threats and help governments against cybercrime. From the outset, the new EU headquarters focused on illegal online activities by organised criminal groups, in particular attacks on electronic banking and other financial activities. The centre provides support for more effective protection of social networking profiles against cybercrime and information and analysis to national law enforcement authorities. Since its inception, the EC3 publishes yearly the Internet Organised Crime Threat Assessment (IOCTA). EC3 has made a significant contribution to the fight against cybercrime by participating in a number of outstanding operations and providing operational support on the ground.[47]

[45] European Commission: *Joint Communication to the European Parliament and the Council. Report on Implementation of the EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 23.6.2021 JOIN(2021) 14 final. 2.

[46] Ibid.

[47] Europol: *European Cybercrime Centre – EC3.* s. a.

Eurojust

According to the Lisbon Treaty, the Eurojust is responsible for supporting and strengthening the coordination and cooperation between national investigating and prosecuting authorities in relation to serious crimes affecting two or more Member States (Article 85). The European Union Agency for Criminal Justice Cooperation (Eurojust) is the successor to the Judicial Cooperation Unit of the European Union created in 2002. The new regulation of Eurojust was adopted in 2018.[48]

The European Judicial Cybercrime Network (EJCN) was established in 2016 to promote "contacts between practitioners specialised in countering the challenges posed by cybercrime, cyber-enabled crime and investigations in cyberspace, and to increase efficiency of investigations and prosecutions". [49]

European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA)

The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA), was established in 2011 (Establishing Regulation (EU) No 1077/2011) and started its activities in 2012. The headquarters of this agency are in Tallinn, Estonia, and its operational centre is in Strasbourg, France. A business continuity site for the systems under management is situated in Sankt Johann im Pongau, Austria and a Liaison Office in Brussels, Belgium.

The EU-Lisa is responsible for the operational management of large-scale IT systems, which are essential instruments in the implementation of the Union's policies in the area of justice, security and freedom. It facilitates the implementation of the asylum, border management and migration policies of the EU.

The Agency is currently providing operational management of the Eurodac (a large-scale fingerprint database mainly for asylum applications), the SIS II (the second generation Schengen Information System) and the VIS (Visa Information System).[50]

[48] Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and Replacing and Repealing Council Decision 2002/187/JHA.

[49] Eurojust: *European Judicial Cybercrime Network.* s. a.

[50] EU-LISA: *EU-LISA. Who We Are.* s. a.

European External Action Service (EEAS)

The European External Action Service manages the diplomatic relations of the European Union conducting CFSP. The EEAS has a central role in the field of cyber diplomacy, strategic communication and the policies concerning cyber defence. This body hosts intelligence and analysis centres dealing with cyber issues as well for civilian and military situational awareness (the Single Intelligence Capability: European Union Intelligence Analysis Centre (INTCEN) and the Military Staff Intelligence Directorate). The Hybrid Fusion Cell was established in 2016 within the EU Intelligence Analysis Centre to improve situational awareness and support decision-making. It gathers and analyses classified and open source information concerning hybrid threats.[51]

European Defence Agency (EDA)

The European Defence Agency was established in 2004 as an intergovernmental agency of the Council of the European Union. The EDA supports the Member States and the Council in their effort to improve defence capabilities through European cooperation. According to the Council conclusion, the EDA aims to develop cyber defence capabilities related to CSDP, to civil–military cooperation and synergies, to raise awareness and to cooperate with relevant international partners.[52]

The EU Approach to Cyber Diplomacy

The EU has started to play an increasingly active role not only in deepening the integration process between its own Member States, but also in resolving international disputes related to cybersecurity and cyber defence.[53] The 2013 strategy set out the EU's international cyber policy. In addition to protecting a free and open Internet, the new policy aimed to promote international law of

[51] European Court of Auditors (2019): op. cit. 50.
[52] Rehrl (2018): op. cit. 93–94.
[53] Thomas Renard: EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain. *European Politics and Society,* 19, no. 3 (2018). 321–337.

responsible state behaviour and confidence-building measures in cyberspace and to improve cooperation with the EU's strategic partners. To this end, negotiations have begun with the United States, China, Japan, South Korea, India and Brazil. During the negotiations, the parties discussed, inter alia, the areas of international security in cyberspace, resilience, cybercrime, Internet governance and cybersecurity standards. An important milestone in 2015 was the adoption of Council conclusions on cyber diplomacy to support the EU's collective efforts.[54]

- EU approach to cyber diplomacy at global level
- promotes and protects human rights and is grounded on the fundamental EU values of democracy, human rights and the rule of law, including the right to freedom of expression, access to information and right to privacy
- ensures that the Internet is not abused to fuel hatred and violence and safeguards that the Internet remains, in scrupulous observance of fundamental freedoms, a forum for free expression in full respect of law
- promotes a cyber policy informed by gender equality
- advances European growth, prosperity and competitiveness and protects EU core values, inter alia, by strengthening cybersecurity and improving cooperation in fighting cybercrime
- contributes to the mitigation of cybersecurity threats, conflict prevention and greater stability in international relations through the use of diplomatic and legal instruments
- promotes the efforts to strengthen the multi-stakeholder model of Internet governance
- fosters open and prosperous societies through cyber capacity building measures in third countries that enhances the promotion and protection of the right to freedom of expression and access to information and that enables citizens to fully enjoy the social, cultural and economic benefits of cyberspace, including by promoting more secure digital infrastructures
- promotes the sharing of responsibilities among relevant stakeholders, including through cooperation between the public and private sectors as well as research and academic institutions on cyber issues[55]

[54] Rehrl (2018): op. cit. 23.

[55] Council of the European Union: *Council Conclusions on Cyber Diplomacy.* Brussels, 11 February 2015 (OR. en).

According to Bendiek "it is a politically and legally controversial issue whether attacked states should adopt offensive countermeasures, such as hack-backs, to neutralise the source of a cyber-attack, […] and the state requires military and strategic cyber weapons as well as a legal basis for their deployment in order to respond to cyberattacks."[56]

At the international level, the EU attached importance to the strict application of international law, in particular the UN Charter and international humanitarian law, and the full implementation of universal non-binding cyber norms, rules and principles of responsible state behaviour in cyberspace for conflict prevention and stability. The EU also promotes the development of confidence building measures and cooperation with other international organisations. According to Rehrl, the OSCE, which is a very important partner of the EU, is the most advanced organisation in the field of confidence-building measures at the regional level.[57]

Due to the growing level of cyber threats and challenges in recent years, cyber diplomacy has become an integral part of Common Foreign and Security Policy. EU Member States agreed on strengthening cyber diplomacy capabilities within the European External Action Service in 2015. The implementation plan on security and defence confirmed this intention in 2016. Important bodies (EU INTCEN and EUMS INT) started to deal with cyber issues.[58]

In 2017, the Council of the European Union agreed to develop a framework for joint EU diplomatic action against malicious cyber activities by state and non-state actors. The so-called Cyber Diplomacy Toolbox was built on the EU's CFSP Policy Toolbox. The EU stands ready to take action on Common Foreign and Security Policy measures, including restrictive measures against activities using information and communication technologies (ICT) that could exhaust the notion of an act of violation of international law.[59]

In line with the EU's cyber diplomatic approach, the joint action will contribute to conflict prevention, the reduction of cybersecurity threats and the enhancement of stability in international relations. The Council set the goal of providing a framework for joint EU diplomatic action to facilitate cooperation,

[56] Annegret Bendiek: The EU as a Force for Peace in International Cyber Diplomacy. *SWP Comment,* no. 19 April 2018. 1–2.

[57] Rehrl (2018): op. cit. 25.

[58] Bendiek (2018): op. cit. 1–2.

[59] Council of the European Union: *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").* Brussels, General Secretariat of the Council, 2017a.

promote risk reduction and influence the behaviour of potential attackers. This EU diplomatic response will make full application of measures used under the Common Foreign and Security Policy, including restrictive measures and possible sanctions. According to the Council conclusions, "a joint EU response to malicious cyber activities would be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity".[60]

On 11 October 2017, the Political and Security Committee adopted implementing guidelines for the Cyber Diplomacy Toolbox. The document listed five categories of measures within the cyber diplomacy toolkit. These included restrictive measures and the procedure for imposing such measures.[61]

According to the 2018 Cyber Defence Policy Framework, the events of previous years have further highlighted the need for more cooperation within the international community in order to prevent conflicts and strengthen the stability of cyberspace.

> "The EU is promoting, in close cooperation with other international organisations, in particular the UN, the OSCE and the ASEAN Regional Forum, a strategic framework for conflict prevention, cooperation and stability in cyberspace, which includes (i) the application of international law, and in particular the UN Charter in its entirety, in cyberspace; (ii) the respect of universal non-binding norms, rules and principles of responsible State behaviour; (iii) the development and implementation of regional confidence building measures (CBMs). The Cyber Defence Policy Framework should also support this endeavour."[62]

In 2019, the EU made significant progress in making the Cyber Diplomacy Toolbox against malicious cyber activities operational and effective. In order to achieve the objectives laid down in its conclusions of June 2018 and October 2018, the European Council decided to introduce EU restrictive measures to help improve the response and deterrence capacity of the Union. On 17 May 2019, a Council Decision [(CFSP) 2019/797] and a Council Regulation [(EU) 2019/796] was taken on restrictive measures against cyberattacks threatening the Union or its Member States.[63] The decision identifies the applicability of measures within the CFSP, if necessary, restrictive measures against malicious cyber activities, and the regulation allows

[60] Council of the European Union: Cyber Attacks: EU Ready to Respond with a Range of Measures, Including Sanctions. *Press Release,* 19 June 2017b.

[61] Council Decision (CFSP) 2019/797 of 17 May 2019, Concerning Restrictive Measures against Cyber-attacks Threatening the Union or its Member States.

[62] Council of the European Union (2018): op. cit. 8.

[63] Council Decision (CFSP) 2019/797.

the EU to impose sanctions as a response to cyberattacks with a significant effect which constitute an external threat to the Union or its Member States.[64]

The new legal framework has thus made it possible for the EU to impose sanctions (e.g. asset freeze, travel ban) to deter and respond to cyberattacks that constitute an external threat to the Union or its Member States. Those sanctions should be effective, proportionate and dissuasive.[65]

In June and October 2020, the Council added several natural and legal persons or entities to the list of natural and legal persons, entities and bodies subject to restrictive measures in accordance with Council Decision (CFSP) 2019/797 in order to prevent, discourage, deter and respond malicious behaviour in cyberspace. The natural or legal persons, entities or bodies named in the Decision are responsible for, providing or supporting cyberattacks, including attempted cyberattacks against the OPCW, cyberattacks known as "WannaCry" and "NotPetya", Operation Cloud Hopper, and the cyberattack on the Federal Parliament of Germany in April and May 2015.[66]

Conclusions

EU decision-makers initially considered the field of digitisation and the use of ICT tools primarily as economic issues. However, the process of securing this area began in early 2010, with the 2013 cybersecurity strategy as a milestone.

In recent years, EU Member States and institutions have continued to be the main targets of cyberattacks and disinformation campaigns. Just a few months after the adoption of measures to sanction serious attacks on the Union and its Member States, a cyberattack on the Bulgarian tax authorities in 2019 resulted in the theft of data from 5 million citizens. In early 2019, the Spanish and Lithuanian Ministries of Defence, as well as the Finnish Ministry of Justice, also fell victim to cyberattacks. In addition to the unprecedented global health crisis, the 2020 coronavirus epidemic has also contributed to the spread and growth of various types of cyberattacks.[67]

[64] Ibid.

[65] European Commission: *Report on the Implementation of the Action Plan Against Disinformation. Joint Communication to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions.* Brussels, 14.6.2019 JOIN(2019) 12 final. 8.

[66] Council Decision (CFSP) 2020/1127; Council Decision (CFSP) 2020/1537.

[67] Daniel Fiott – Vassilis Theodosopoulos: *Yearbook of European Security.* EUISS, 2020.

References

Bendiek, Annegret: *The EU as a Force for Peace in International Cyber Diplomacy. SWP Comment,* no. 19 April 2018. Online: www.swp-berlin.org/fileadmin/contents/products/comments/2018C19_bdk.pdf

Council Decision (CFSP) 2019/797 of 17 May 2019, Concerning Restrictive Measures against Cyber-attacks Threatening the Union or its Member States. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019D0797&from=EN

Council Decision (CFSP) 2020/1127 of 30 July 2020, Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyber-attacks Threatening the Union or its Member States. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=HU

Council Decision (CFSP) 2020/1537 of 22 October 2020 Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyber-attacks Threatening the Union or its Member States. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1537&from=EN

Council of the European Union: *Report on the Implementation of the European Security Strategy. Providing Security in a Changing World.* Brussels, 11 December 2008. Online: www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/reports/104630.pdf

Council of the European Union: *European Security Strategy. A Secure Europe in a Better World.* Brussels, General Secretariat of the Council, 2009. Online: https://doi.org/10.2860/1402

Council of the European Union: *Internal Security Strategy for the European Union. Towards a European Security Model.* Brussels, General Secretariat of the Council, 2010. Online: https://doi.org/10.2860/87810

Council of the European Union: *EU Cyber Defence Policy Framework.* Brussels, 18 November 2014. Online: www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf

Council of the European Union: *Council Conclusions on Cyber Diplomacy.* Brussels, 11 February 2015 (OR. en). Online: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf

Council of the European Union: *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").* Brussels, General Secretariat of the Council, 2017a. Online: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

Council of the European Union: Cyber Attacks: EU Ready to Respond with a Range of Measures, Including Sanctions. *Press Release,* 19 June 2017b. Online: www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

Council of the European Union: *EU Cyber Defence Policy Framework, (as updated in 2018).* Brussels, 19 November 2018(OR. en). Online: http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

Council of the European Union: *Permanent Structured Cooperation (PESCO)'s Projects – Overview.* 2019. Online: www.consilium.europa.eu/media/39762/pesco-overview-of-first-collaborative-of-projects-for-press.pdf

Council of the European Union: *Draft Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 9 March 2021(OR. en). Online: https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf

Council of the European Union: Bucharest-based Cybersecurity Competence Centre Gets Green Light from Council. *Press Release,* 20 April 2021. Online: www.consilium.europa.eu/en/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/

Council Regulation (EU) 2019/796 of 17 May 2019, Concerning Restrictive Measures against Cyber-attacks Threatening the Union or its Member States. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0796&from=EN

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. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

ENISA: *About ENISA – The European Union Agency for Cybersecurity.* s. a. Online: www.enisa.europa.eu/about-enisa

ENISA: *CSIRTs Network.* s. a. Online: www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

EU Cyber Direct: *Cyber-related PESCO Projects.* Brussels, 12 November 2019. Online: https://eucyberdirect.eu/content_knowledge_hu/cyber-related-pesco-projects/

EU-LISA: *EU-LISA. Who We Are.* s. a. Online: www.eulisa.europa.eu/About-Us/Who-We-Are

Eurojust: *European Judicial Cybercrime Network.* s. a. Online: www.eurojust.europa.eu/Practitioners/Pages/EJCN.aspx

European Commission: Brussels, 1.6.2005, COM(2005) 229 final, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions "i2010 – A European Information Society for growth and employment". Commission of the European Communities, 2005. Online: lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:EN:PDF

European Commission: *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* JOIN/2013/01 final. Online: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf

European Commission: *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe.* Brussels, 6.5.2015, COM(2015) 192 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

European Commission: *Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU.* Brussels, 13.9.2017, JOIN(2017) 450 final. Online: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX-%3A52017JC0450

European Commission: *State of the Union 2017 – Cybersecurity: Commission Scales Up EU's Response to Cyber-attacks.* Brussels, 19 September 2017. Online: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193

European Commission: *Shaping Europe's Digital Future. Policy, European Cybersecurity Industrial, Technology and Research Competence Centre.* Brussels, 19 September 2018. Online:

https://ec.europa.eu/digital-single-market/en/european-cybersecurity-industrial-technology-and-research-competence-centre
European Commission: *Report on the Implementation of the Action Plan Against Disinformation. Joint Communication to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions.* Brussels, 14.6.2019 JOIN(2019) 12 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019JC0012&from=EN
European Commission: *Shaping the Digital Single Market.* 2020. Online: https://ec.europa.eu/digital-single-market/en/europe-2020-strategy
European Commission: *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 16.12.2020 JOIN(2020) 18 final. Online: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
European Commission: *Joint Communication to the European Parliament and the Council. Report on Implementation of the EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 23.6.2021 JOIN(2021) 14 final. Online: https://digital-strategy.ec.europa.eu/en/library/first-implementation-report-eu-cybersecurity-strategy
European Commission: *The Digital Europe Programme.* s. a. Online: https://digital-strategy.ec.europa.eu/en/activities/digital-programme
European Commission: *Departments and Executive Agencies.* s. a. Online: https://ec.europa.eu/info/departments
European Council: *European Council Conclusions 19/21 December 2013.* Online: www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/140245.pdf
European Court of Auditors: Challenges to Effective EU Cybersecurity Policy. *Briefing Paper,* March 2019. Online: www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf
European External Action Service: *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy.* 2016. Online: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf
Europol: *European Cybercrime Centre – EC3.* s. a. Online: www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
Fiott, Daniel – Vassilis Theodosopoulos: *Yearbook of European Security.* EUISS, 2020. Online: www.iss.europa.eu/sites/default/files/EUISSFiles/YES_2020.pdf
Kovács, László: *Kiberbiztonság és stratégia.* Budapest, Dialóg Campus, 2018.
Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and Replacing and Repealing Council Decision 2002/187/JHA. Online: www.eurojust.europa.eu/hu/document/regulation-eu-20181727-14-november-2018-european-union-agency-criminal-justice-cooperation
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) PE/86/2018/REV/1. Online: https://eur-lex.europa.eu/eli/reg/2019/881/oj

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), Article 1(1). Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0526

Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 Establishing the Digital Europe Programme and Repealing Decision (EU) 2015/2240 (Text with EEA Relevance). Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A32021R0694

Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 Establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. Online: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32021R0887

Rehrl, Jochen (ed.): *Handbook on Cybersecurity. The Common Security and Defence Policy of the European Union.* Luxembourg Publications Office of the European Union, 2018. Online: https://doi.org/10.2855/3180

Renard, Thomas: EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain. *European Politics and Society,* 19, no. 3 (2018). 321–337. Online: https://doi.org/10.1080/23745118.2018.1430720