Computer Law & Security Review 55 (2024) 106055

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

Collective cyber situational awareness in EU. A political project of difficult legal realisation?

Federico Serini

Economics and Law Department, La Sapienza University, 00185, Rome, Italy

ARTICLE INFO

Keywords:
European Union Law
European cybersecurity
Cyber situational awareness
Cybersecurity information sharing

ABSTRACT

From 2020 onward, the European cybersecurity strategy has seen a major reformulation of its objectives given the changed international environment. The policy documents reveal an interest in the establishment of an increasingly integrated overall security system, in which the relevant institutions of the Union have a central role. Among the various aspects considered is the establishment of a "collective situational awareness" based on the exchange of security information between Member States and European authorities, as well as between the Union authorities themselves. The sharing of security information is certainly an expression of the capacity for cooperation among Member States in the "Area of Freedom, Security and Justice" of the European Union. The analysis proposed in this contribution aims to study the organisation and procedures of information exchange to counter cyber threats (cybersecurity information sharing) in light of recent legislative interventions in the field of cybersecurity. After analysing the evolution of European administrations, and the tools employed in cybersecurity information sharing practices, the investigation focuses on the dynamic profiles related to the treatment of personal data and sensitive and classified information contained in said information by the different actors involved in the sharing process (private entities, single points of contact, law enforcement agencies, European institutions). The conclusions aim to formulate some considerations on the current state of the art in cybersecurity information sharing practices.

This paper takes part from a previous article, written in Italian, which title is "*Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche. Verso una definizione di cybersicurezza integrata?*" (The European Information Cooperation System for Countering Cyber Threats. Towards an integrated cybersecurity definition?), published on MediaLaws Review n. 3, 2023, pp. 144-187.

1. Cyber situational awareness in the EU dimension

Situational Awareness (SA) is closely linked to human cognition and the way humans perceive the environment. This is why this process has been studied from different disciplinary perspectives, making it difficult to systematise it on a scientific level.

The definition generally referred to is provided by strategic literature. Mica R. Endsley, the Chief Scientist of the U.S. Air Force, defines it as a three-stage process: «[p]erception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in near future».[1] In other words, it is a process articulated in recognition, situation comprehension, and situation projection steps, that enables decision-makers to assess the best choice to be made considering the overall context and the associated variables of risk, danger and future damage about a threat event.[2]

Cyber Situational Awareness (CSA) is a branch of the traditional situational awareness just described that - precisely - finds application in the context of cyberspace to protect cyber assets, make better cyber

E-mail address: federico.serini@uniroma1.it.

[1] M.R. Endsley, *Design and evaluation for situation awareness enhancement*, Proceedings of the Human Factors Society annual meeting, vol. 32, 1988, 97, available at https://journals.sagepub.com/doi/10.1177/154193128803200221. See also the definition provided by the Glossary of the National Institute of Standards and Technology (NIST), which defines SA as follows: «[w]ithin a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future», available at https://csrc.nist.gov/glossary/term/situational_awareness.

[2] Some have proposed using other model as the Observe – Orient – Decide – Act (OODA) loop, see J. Pöyhönen, J. Rajamäki, R. Harri, L. Martti, *Cyber Situational Awareness in Critical Infrastructure Protection*, Annals of Disaster Risk Sciences, vol. 3, n. 1, 2020, available at https://hrcak.srce.hr/file/362954.

https://doi.org/10.1016/j.clsr.2024.106055

Available online 23 September 2024

security decisions and improve security functions and organisation.[3]

Specifically, the CSA process is fed by an information pool consisting of data from cyber sensors (mostly intrusion detection systems), as well as information from analysis processes conducted from different perspectives (e.g. cyber threat analysis, threat intelligence analysis, geopolitical analyst considerations, etc.), subsequently disseminated within the sharing systems. This last activity is called "cyber threat information sharing" and consists of the «exchange of a variety of network and information security related information such as risks, vulnerabilities, threats and internal security issues as well as good practice».[4]

The European cyber-security administrative structure has developed over time through the establishment of several decentralised coordinating bodies, organised mostly on the model of agencies with legal personality, which find in the exchange of information between them, as well as with the competent authorities of the Member States, the essential element for their functions.

Despite efforts to establish an administrative and regulatory framework for information sharing, i.e. the NIS discipline, in the European Cyber Security Strategy presented in December 2020, it is reported that «[t]he EU lacks collective situational awareness of cyber threats».[5] According to the Commission, the problem is due, on the one hand, to the low involvement of the private sector in information cooperation and, on the other hand, to the resistance of the Member States to share information systematically and comprehensively, thus making the functioning of cyber information sharing mechanisms between the Member States and EU institutions extremely difficult in the event of large-scale cross-border cyber incidents or crisis.[6]

European Commission President Ursula von der Leyen herself, in her "State of the Union 2021″, reiterated the need to «build the foundation for collective decision-making», this is what she calls «situational awareness», based on the exchange of knowledge «from all services and all sources. From space to police trainers, from open source to development agencies».[7] Again, she noted that «[w]e have knowledge, but it is disjointed. Information is fragmented», calling for the creation of a Joint Situational Awareness Centre to merge all the different information «[t]o be better prepared, to be fully informed and to be able to make decisions».[8]

As has been noted,[9] the attention of doctrine towards this topic is still scarce and fragmented, and we would like to add, that the few studies that have been conducted mostly concern the cyber situational awareness process from the perspective of individual organisations.[10]

This clarification is necessary because, in the aforementioned Strategy and the recalled Speech of the President of the Commission, the European Union referred to a "collective decision-making" process which involves all Member States and not just the individual organizations.[11] That is why we believe that in the Union's plans, there is an intention to create a process of Collective cyber situational awareness (CCSA) as strategic direction, with related legal and organisational-administrative repercussions.

Considering that the establishment of the Joint Situational Awareness Centre is still under discussion,[12] with this contribution we propose to investigate the state of the art regarding the possible implementation of CCSA systems at the European level, and to do so we will conduct the study from the perspective of the first phase of situational awareness processes: cybersecurity information sharing.

The 2020 World Economic Forum report identified seven barriers "that need to be overcome" to the progress of greater information that will support the security and resilience of the global economy.[13] The challenges listed in the document are gaps in jurisdictions and cross-sector collaboration; lack of skills and capabilities; lack of privacy and trust in the sharing systems; lack of alignment and harmonization across jurisdictions; operational, interoperability and technology barriers; operational costs and lack of clear incentives (these were also highlighted in an ENISA document from 2010[14]).

We believe that some of these issues do not exist at the European level such as jurisdictional gaps, lack of economic and organizational capabilities, and absence of policies and legislation in this regard. However, establishing a process of CCSA in the EU may certainly pose other types of challenges related to establishing appropriate administrative structures, a legislative framework that promotes information sharing, as well as the use of interoperable technologies to promote the sharing of cybersecurity information among Member States.

We will analyse the topic from a twofold perspective: static, relating to the study of the European cybersecurity information sharing architecture (para. 2), reflecting on the role of NIS actors in this process (para. 3), the establishment of public-private partnerships for the sharing (para. 4) and also the technical tools use for it (para. 5); and dynamic from the data law perspective, focusing on the practice of cyber information sharing between private and public actors (including police forces), in the light of the relative bases of legitimacy justifying the traffic of both personal data and "sensitive and classified" information contained in cybersecurity information (para. 6).

2. The European cybersecurity information sharing organizations

Among the activities functional to the process of European integration,[15] the exchange of information between the various Member States, as well as between the latter and the European institutions, has become increasingly important to foster the coordination of the Union's administrative activities under the principles of loyal cooperation, as recognised in Article 4(3) of the Treaty on European Union (TEU), and subsidiarity, as recognised in Article 5 TEU.

In the specific case of security policies, the exchange of information between the police and intelligence authorities of the Member States, and between them and the European institutions, is an activity that takes on particular relevance as an expression of the Member State's ability to

[3] On the different definitions of the concept of Cyber Situational Awareness, see S. Jajodia, P. Liu, V. Swarup, C. Wang, *Cyber situational awareness*, Springer Science & Business, 2009, available at https://link.springercom/book/10.1007/978-1-4419-0140-8.

[4] N. Robinson, E. Disley, *Incentives and Challenges on Information Sharing. Retrieved*, 2010, p. 9, available from the ENISA website at https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing.

[5] JOIN(2020) 18 final, *Joint Communication to the European Parliament and the Council, the EU's Cybersecurity Strategy for the Digital Decade*, p. 3, available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX/3A52020JC0018.

[6] Ibid, p. 4.

[7] U. von Der Leyen, 2021 State of the Union, *Strenghtening the soul of our Union*, Strasbourg, 15 September 2021.

[8] Ibid.

[9] U. Franke, J. Brynielsson, *Cyber situational awareness – A systematic review of the literature*, Computer & Security, vol. 46, 2014, pp. 18-31, available at https://www.sciencedirect.com/science/article/pii/S0167404814001011.

[10] A. Horneman, *Situational Awareness for Cybersecurity: An Introduction*, Carnegie Mellon University, Software Engineering Institute's Insights (blog), 2019, last accessed November 22, 2023, available at https://insights.sei.cmu.edu/blog/situational-awareness-for-cybersecurity-an-introduction/.

[11] U. von Der Leyen, 2021 State of the Union.

[12] Parliamentary question - E-004266/2021(ASW), 26.1.2022.

[13] World Economic Forum, *Cyber Information Sharing: Building Collective Security*, insight report, october 2022, available at https://www.weforum.org/publications/cyber-information-sharing-building-collective-security/.

[14] N. Robinson, E. Disley, *Incentives and Challenges on Information Sharing. Retrieved …op. cit.*.

[15] G. de Búrca, J.H.H. Weiler, *The worlds of European constitutionalism*, New York, 2012.

cooperate as a founding element of the European Union's Area of Freedom, Security and Justice.[16]

As learned from the new European security policy, the "*Security Union Strategy 2020–2025*", the topic has been the subject of recent attention from the Union given the reference to the fact that:

> [a] although the primary responsibility for security lies with the individual Member States, it has become clear in recent years that the security of one Member State is the security of all. The EU can bring a multidisciplinary and integrated response, providing security actors in the Member States with the tools and information they need.[17]

As is well known, the European security system has developed over time on the logic of intergovernmental cooperation, never finding full communitarisation. See the clauses in the Treaties protecting "national security" or "public order and security" that suspend its application in favour of Member State prerogatives.[18]

These prerogatives that centralise the role of States have not precluded the subsequent development of policies and the creation of common institutions to guarantee the need for security throughout the European space. Observing the historical evolution of cooperation between European States in the police sector, one realises that it is precisely in the collection, storage, processing and exchange of information that the integration process in this area finds concrete realisation.[19]

In particular, Information sharing has fundamental importance in the context of cyberspace security. Network systems and ICT goods have a vulnerable nature because it was not developed originally with the idea of being secure from the malicious activities of others.

Widespread vulnerabilities that require equally widespread readiness and response capabilities are possible only through the prompt dissemination of information following malicious events. Information acquired after a cyber attack is indeed useful for enhancing defences, conducting investigations by professionals, and providing a clear picture of the situation to the decision-maker. Reason why cybersecurity information sharing has been codified as a principle at the international level by some economic organizations.[20]

Based on this, the European cyber-security administrative structure has developed over time through the establishment of several decentralised coordinating bodies, organised mostly on the model of agencies with legal personality, which find in the exchange of information between them, as well as with the competent authorities of the Member States, the essential element for their functions.

In 2004, there has been the European Cybersecurity Agency (ENISA), established to create «confidence under its independence, the quality of the advice it delivers and the information it disseminates, the transparency of its procedures and methods of operation, and its diligence in performing the tasks assigned to it» and «[a]s electronic networks, to a large extent, are privately owned, the Agency should build on the input from and cooperation with the private sector» (Recital 11). The agency was initially given a temporary mandate, which Regulations gradually extended (EU) No. 1007/2008, and No. 580/2011. However, it was only with Regulation 2019/881, the Cybersecurity Act, that ENISA was given a permanent mandate, strengthening its role, tasks and responsibilities, and providing more resources to help support Member States in preventing and responding effectively to cyber attacks.

In particular, the Agency acts as the secretariat of the network composed of the national intervention teams (the CSIRT network) and supports operational cooperation between them and the Union's intervention team, CERT-EU, which has the function of responding efficiently to cyber threats directed against the Union's networks and institutional systems.

[16] See Title V of the TFEU entitled "Area of freedom, security and justice". In the list of the main legislative acts on police cooperation available on the website of the European Parliament, it appears that a large part of these are aimed at establishing communication mechanisms to facilitate the exchange of information between member states, see Directive (EU) 2016/681 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime; Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters; Regulation (EU) 2019/818 establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration; Directive (EU) 2019/1153 laying down provisions to facilitate the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences; and Regulation (EU) 2021/784 on countering the dissemination of terrorist content online, applicable from 7 June 2022.

[17] The EU Security Union Strategy 2020-2025, COM(2020) 605 final, del 24 luglio 2020.

[18] It is worth recalling the content of Article 4(2) of the Treaty on European Union (TEU) where it is stipulated that «The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect its essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State». This permanent state competence clause, added at the explicit request of the United Kingdom, must also be read in conjunction with Art. 276 of the Treaty on the Functioning of the European Union (TFEU), which excludes review by the Court of Justice of the «validity or proportionality of operations carried out by the police or other law-enforcement services of a Member State or the exercise of the responsibilities incumbent upon Member States about the maintenance of law and order and the safeguarding of internal security».

[19] In the list of the main legislative acts on police cooperation available on the website of the European Parliament (referred to at https://www.europarl.europa.eu/factsheets/en/sheet/156/cooperazione-di-polizia consulted on 26 June 2024), it appears that a large part of these are aimed at establishing communication mechanisms to facilitate the exchange of information between Member States. See Directive (EU) 2016/681 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime; Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters; Regulation (EU) 2019/818 establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration; Directive (EU) 2019/1153 laying down provisions to facilitate the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences; and Regulation (EU) 2021/784 on countering the dissemination of terrorist content online, applicable from 7 June 2022.

[20] Reference Guidelines for the Security of Information Systems by the Organisation for Economic Cooperation and Development (OECD) in 2002, available at https://www.oecd.org/digital/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm, where nine principles were elaborated including those of «(3) Response: Interested parties must work promptly and in a spirit of cooperation to prevent, detect and respond to security incidents [...]»; «(8) Security management: Interested parties must adopt a comprehensive approach to security management [...]»; «(9) Reassessment: Interested parties must examine and reassess the security of information systems and networks and introduce appropriate changes in their security policies, practices, actions and procedures [...]».

CSIRTs, acronyms of Computer Security Incident Response Teams, are decentralised intervention units, established in individual Member States (possibly also within competent authorities[21]), with the task of carrying out reactive activities, such as intervention in the event of a cyber incident, and proactive activities, such as monitoring incidents at a national level, issuing early warnings, alerts, announcements and dissemination of information to interested parties about risks and incidents, and analysing these risks and incidents.

In both cases, these actors represent the central nerve of cyber information sharing processes. On one hand, they receive information on cyber threats from NIS entities; on the other hand, they participate in the broader information cooperation at the European level through the network that brings together representatives of all Member States' intervention teams and the CERT-EU team, under the secretariat of ENISA (the CSIRT network.

This activity is also supported by the "Cooperation Group", a body composed of representatives of the Member States, the Commission and ENISA, whose function is to facilitate strategic cooperation and the exchange of information between Member States by providing guidance and advice to the European institutions, as well as by conducting coordinated cyber-security risk assessments and producing reports useful for the Commission's review of the NIS framework.[22]

On January 2023 came into force the Directive (EU) 2022/2555 (NIS II Directive),[23] which repealed the former Directive (EU) 2016/1148 (NIS I Directive).

The European legislator, with this new regulation, wanted to improve the dissemination of cybersecurity information establishing the "EU Cyber Crisis Liaison Organisation Network" (CyCLONe), a closer cooperation and coordinated action in cases of large-scale cyber security incidents. To this end, the Network supports the coordinated management of large-scale cyber security incidents and crises at an operational level and ensures the regular exchange of relevant information between the Member States and the Union institutions, bodies, offices and agencies.[24]

Since June 2023, the Joint Cyber Unit is also operational. It is a connecting platform where participants from the civil, diplomatic, law enforcement and defence communities can draw on each other's support and expertise, especially when the various communities have to work closely together in large-scale incidents or crises.[25] The Unit does not constitute an additional independent body but is the result of the provision of a physical common space, located in Brussels, and a virtual space composed of useful tools for secure and rapid information sharing.

The participating European administrations include law enforcement, the European Cybercrime Centre (EC3), a specialised unit already established within EUROPOL with liaison functions with the police forces of European States[26]; on the diplomatic level, the European External Action Service (EEAS)[27] and the *Horizontal Working Party on Cyber Issues*[28]; finally, as regards the defence sector, the Permanent Structured Cooperation (PESCO) framework[29] and the *European Defence Agency* (EDA).[30]

Is pending approval by the European Parliament a proposal for a regulation made by the Commission in April 2023 establishing a set of measures to strengthen solidarity and capabilities to detect, prepare for and respond to cyber security threats and incidents in the European context, the EU Cyber Solidarity Act.[31]

With this instrument, the Union intends to increase situational awareness, and information sharing, and improve cyber incident preparedness and response at a common level through the establishment of three new interlocking mechanisms: the European Cybersecurity Shield, the Cyber Emergency Mechanism and the Cybersecurity Incident Review Mechanism.

The European Cybersecurity Shield will be tasked with improving the detection, analysis and response to large-scale cyber threats through the establishment of a new network of multinational Security Operation Centres SOC platforms. The first phase of the project has already been launched in November 2022, and three consortia of cross-border Security Operation Centres (SOCs), bringing together public bodies from 17 Member States and Iceland, have been selected within the framework of the Digital Europe programme (par. 5.1 on SOCs).

The Cyber Emergency Mechanism will have the task of improving preparedness and response to cyber security incidents through the evaluation of response mechanisms implemented in particularly critical sectors selected at the end of a general EU-wide risk assessment; the creation of the EU Cybersecurity Reserve, i.e. incident response services provided by private service providers ("trusted providers"), activated at the request of Member States or EU institutions, to help them address significant problems or large-scale cyber security incidents: and by

[21] This is for example the case of the CSIRT Italy transferred to Agenzia Nazionale per la Cybersicurezza (ACN) with Decree-Law No. 82 of 2021.

[22] Art. 12 NIS I. Directive.

[23] Directive (UE) 2022/2555, on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS II Directive).

[24] Art. 16 NIS II Directive.

[25] C(2021) 4520 *final*, *on building a Joint Cyber Unit*, 2021, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX/3A32021H1086. On closer inspection, the Joint Cyber Unit builds on the previous 2017 Blueprint project established by Recommendation (EU) 2017/1584 on a coordinated response to large-scale cybersecurity incidents and crises.

[26] The European Cybercrime Centre (EC3) is a body established by Europol in 2013, based in The Hague. Its activity is to coordinate cross-border cybercrime law enforcement activities and serves as a centre of technical expertise in the field. For further information, please refer to the official website at https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

[27] The European External Action Service (EEAS) is the EU's diplomatic service, set up to make EU foreign policy more coherent and effective and thus strengthen Europe's influence on the world stage. For more information, see the official website at https://www.eeas.europa.eu/_it.

[28] The Forum Horizontal Working Party on Cyber Issues was established in 2016 and is responsible for coordinating the Council's work on cyber issues, mainly cyber policy and legislative activities. The Working Party cooperates closely with the European Commission and other institutions such as the European External Action Service, Europol, Eurojust, the European Fundamental Rights Agency (FRA), the European Defence Agency (EDA) and the European Union Agency for Cyber Security (ENISA).

[29] The Permanent Structured Cooperation (PESCO) in the field of security and defence policy was established on 11 December 2017 by Council Decision 2017/2315. This instrument provides a legal framework to jointly plan, develop and invest in shared capability projects and improve the operational readiness and contribution of armed forces.

[30] The European Defence Agency was established by a Joint Action of the Council of Ministers on 12 July 2004, «to support the Member States and the Council in their effort to improve European defence capabilities in the field of crisis management and to sustain the European Security and Defence Policy as it stands now and develops in the future», see at the website https://eda.europa.eu/who-we-are/Missionandfunctions.

[31] COM(2023) 209 final, proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents.

promoting mutual assistance between Member States when one of them has been affected by a cyber security incident.[32]

3. Cyber information sharing in light of the NIS II Directive

The transboundary nature of cyber threats has characterized cybersecurity organizations with an increased need to resort to information cooperation mechanisms through the establishment of exchange networks among entities that mutually trust each other.[33]

In addition to the competent public authorities in policing, intelligence, and defence (as is the case for security in the traditional sense), participants in information exchange in this sector also include the beneficiaries of cybersecurity assurances, mostly represented by public or private entities operating in critical sectors.

Such actors are now governed by the aforementioned Directive (EU) 2022/2555 (NIS II Directive), which in Art. 1, para. 2, lett. c) - unlike the previous legislation - expressly states that the Directive establishes «rules and obligations on cybersecurity information sharing».

The introduction of the concepts of «near miss», «incident» ed «large-scale cybersecurity incident» which are defined in Art. 6 of the NIS II Directive, as well as the concept of significant incident mentioned in Art. 23, para. 3, suggests the different degrees of intervention and management of cyber risk by the entities involved in the European cybersecurity process.[34] This regulation must also be interpreted in the light of the mentioned EU Cyber Solidarity Act, as a tool aimed at enhancing the unified management of widespread impact incidents in the European space.

As anticipated (par. 2), the recent NIS II discipline has integrated the coordinated response system to large-scale cybersecurity incidents and crises established with Recommendation (EU) 2017/1584 of September 13, 2017, including the EU-CyCLONe, the Cooperation Group, and the Network of Intervention Groups. It reaffirms the need for all actors to «specify the arrangements through which that network should function, including the network's roles, means of cooperation, interactions with other relevant actors and templates for information sharing, as well as means of communication».[35]

The scalability of cybersecurity incidents allows us to distinguish between normal information-sharing practices for cybersecurity reasons falling within the definition of cyber information sharing and information exchange activated in the event of an emergency following a significant incident involving an «essential» or «important» entities, or in the case of a large-scale incident. Specifically, regarding this discussion, the interest is to analyze these information circuits from the perspective of those who feed and generate information traffic following an incident.

In case of incidents involving entities classified as «essential» or «important», there is an obligation to report to the competent authorities and/or CSIRT as per Art. 23. Conversely, if the incident involves "other entities" than those just mentioned, the informational compliance with the competent authorities will consist of a «voluntary notification of relevant information» regulated by Art. 30, para. 1, lett. b).

In addition to these emergency procedures, other information circuits fall within the activities of true cyber information sharing. This procedure differs from the first in two ways: 1) the fact that the interaction of these entities occurs not only with the relevant European institutions but also with other NIS actors (mostly belonging to the same sector, e.g., energy, finance, etc. or not), 2) the fact that there are no obligations to participate in information ecosystems. This circuit is fueled by the exclusive will of the participants, whether they are of critical relevance according to the Directive («essential» or «important») or different.[36]

The (voluntary) sharing of information, therefore, takes place based on agreements between the parties. On this matter, the recent NIS II Directive has introduced Art. 29, titled "Cybersecurity information-sharing arrangements". As stated, the European legislator has set the goal for Member States to enable all entities, whether critical or not, to «to exchange on a voluntary basis relevant cybersecurity information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks». In the second paragraph, is specified that such exchange should «implemented through cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information shared» and, in particular, that Member States, in facilitating the conclusion of such agreements, «may specify operational elements, including the use of dedicated ICT platforms and automation tools, content and conditions of the information-sharing arrangements», and in the case of the participation of public authorities in such agreements «may impose conditions on the information made available by the competent authorities or the CSIRTs».

4. The European public-private partnerships in cybersecurity

The Weberian paradigm that sees the State as the sole holder of the legitimate use of force is no longer consistent with the current situation. The process of globalisation has led to a re-articulation of the State that has de facto transferred some of its functions to private actors,[37]

[32] On the concept of "mutual assistance", Art. 10(c) of the EU Cyber Solidarity Act merely refers back to the same notion as in the NIS II Directive. Given the doctrine's interpretative contrasts on the qualification of cyber attack as an armed attack, as well as the state of the art regarding the definition of a European security and defence policy (see A. Deighton, *The European Security and Defence Policy*, JCMS Journal of Common Market Studies, Vol. 40, n. 4, 2022, pp. 719-741, available at https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-5965.00395), it cannot be ruled out that this principle can be traced back to the mutual assistance principle of the same name in Art. 42 TEU, where it is provided that in compliance with the security and defence policy of "certain Member States" assistance to the attacked state is conditional on the prior involvement of NATO.

[33] On cooperative and coordination mechanisms for cybersecurity purposes v. F. Skopik, G. Settanni, R.Fiedler, *A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing*, Computers & Security, 60, 2016, pp. 154-176, available at https://www.sciencedirect.com/science/article/abs/pii/S0167404816300347.

[34] Art. 6, nn. 5, 6, 7 NIS II Directive whereby «near miss» it is mean «an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialise»; about «incident», «an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems»; and finally «large-scale cybersecurity incident» it is mean «an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States».The notion of the significant incident is instead introduced in Art. 23, para 3 of the Directive, titled "Reporting Obligations", which defines it as an incident that «a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned; (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage».

[35] Recital 68, NIS II Directive.

[36] Reference is made to Recital 29 of the Cybersecurity Act, where it is stipulated that «ENISA should support information sharing within and among sectors [...] by providing best practices and guidance on available tools and on procedure, as well as by providing guidance on how to address regulatory issues related to information sharing, for example through facilitating the establishment of sectoral information sharing and analysis centres».

[37] S. Sassen, *Territory, Authority, Rights: From Medieval to Global Assemblages*, Princeton University Press, Princeton, 2008.

including, over time, that of security.[38]

According to some, this process has not seen the full affirmation of the private sector in this area, but rather the establishment of hybrid forms of governance, characterised by close collaboration (i.e. cooperation) with the public power, the result of which has led to the so-called global security assemblages, i.e. the formation of new security structures and practices that are both public and private, as well as global and local.[39]

At the European level,[40] the public-private partnership has proven to be the most suitable tool for ensuring the cybersecurity of sectors qualified as critical, especially in developing European prevention, preparedness, and response to acts of cyberterrorism through the establishment of the Critical Infrastructure Warning Information Network (CIWIN).[41]

The convenience regarding the use of this tool in the specific context of cybersecurity, as well as the protection of critical infrastructure, has been identified by some for the following reasons: «(a) the private sector 'owns or controls' a large number of CIs [critical infrastructures]; (b) the implementation of security policies depends on the involvement of the private sector in the 'definition of strategic public policy objectives as well as operational priorities and measures'; (c) PPPs 'would bridge the gap between national policy-making and operational reality on the ground'».[42]

It is important to note that these initial cooperative experiences arose at the initiative of governments, but their actual realisation and participation occurred solely due to the will of the entities involved (the so-called "bottom-up" approach). Sector-specific self-organization took place according to the operational areas of critical infrastructure (there are ISACs in the financial, and energy sectors, etc.). The dissemination of information and alerts about cyber threats occurred based on private agreements.

At that time, the European Community initially focused on promoting the establishment of these centres at the national level (a need that remains relevant given recent prompts), recognizing «the importance of multi-stakeholder models such as Public Private Partnerships (PPPs), built on a long term, bottom-up model to mitigate identified risks where such an approach delivers added value in helping to ensure a high level of network resilience».[43] Similarly, ENISA, after the implementation of the NIS framework, has produced documents on cooperative models for establishing national ISACs.[44]

However, given the increasingly recognized need to coordinate information and alert exchange procedures uniformly, the Union has also taken steps to create partnerships at the European level. An example is the European Information Sharing and Alerting System (EISAS),[45] a project initiated in 2007 to bridge the gap in information sharing through the study of analysis models and dissemination of cybersecurity information useful for creating a common sharing space.[46]

The European Public-Private Partnership for Resilience - EP3R represented the first attempt to establish a common partnership at the European level to address security and resilience issues in the telecommunications sector.[47] The project, initiated in 2009, was subsequently closed in 2013. Some scholars have attributed the reasons for the failure of this experience to the low participation of project members on various fronts: lack of commitment to information sharing, procedural opacity, and limited involvement of small and medium-sized infrastructures, unlike larger ones directly affected by the NIS framework.[48]

The sharing of information on cyber threats and alerts through the establishment of cooperative structures such as partnerships remains a priority for European cybersecurity policies. Despite the failure of the EP3R, the European Cybersecurity Strategy of 2013 reiterated that «the European Public-Private Partnership for Resilience (EP3R15) is a sound and valid platform at EU level and should be further developed».[49] To this end, within the NIS platform framework, ENISA has created three working groups, with a specific focus on co-regulation tools and related public policies regarding risk management, information sharing, and coordination in the event of incidents between public and private actors. These working groups have replaced the EP3R.

In the same year, the European Commission acknowledged the need to establish the specialized unit EC3 (European Cybercrime Centre) to combat cybercrime at Europol. It is a case of a public-private partnership where among the parties, there are authorities performing policing tasks. Specifically, as learned from the website, EC3 utilises two consultation groups that include private sector actors to create a cooperative environment capable of addressing challenges related to cybercrime, promoting collaboration at both strategic and operational levels.[50]

Building on these groups, EC3 has signed several Memoranda of Understanding (MoU) with private sector entities operating in critical sectors, such as the financial sector,[51] But especially those active in the cybersecurity services sector.[52] These agreements, although an expression of private negotiation, have had the effect of directing the parties towards public purposes and common models of cybersecurity information sharing. On one hand, they have helped the private sector raise security levels, and on the other, they have allowed EC3 to stay updated on the latest cyber threats.[53]

[38] R. Abrahamsen, A. Leander, *Handbook of private security studies*, Routledge, London, 2016.

[39] R. Abrahamsen, M. C. Williams, *Security Privatization and Global Security Assemblages*, The Brown Journal of World Affairs, vol. 18, n. 1, 2011, p. 171.

[40] O. Bures, *Contributions of Private Businesses to the Provision of Security in the EU: Beyond Public-Private Partnerships*, in O. Bures, H. Carrapico (edit by), *op. cit.*, p. 32.

[41] We refer to the CIWIN page available at https://home-affairs.ec.europa.eu/networks/critical-infrastructure-warning-information-network-ciwin_en.

[42] F. Cappelletti, L. Martino, *Achieving Robust European Cybersecurity through Public–Private Partnerships: Approaches and Developments*, EU Policy Review, vol. 1, 2021, p. 62.

[43] European Council, *Council Resolution on a collaborative European approach to network and information security*, 2009/C 321/01, 2009, section IV, 7.

[44] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models,* 2018, available at https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models.

[45] ENISA, *EISAS – European Information Sharing and Alerting System*, 2007, available at https://www.enisa.europa.eu/publications/eisas-report-on-implementation-enhanced/at_download/fullReport; as well as the report, *EISAS (enhanced) report on implementation,* published in 2011 and available at https://www.enisa.europa.eu/publications/eisas-report-on-implementation-enhanced.

[46] For information on the various critical sectors involved in the EISAS circuit, please refer to https://www.isacs.eu/european-isacs.

[47] ENISA, *EP3R 2009-2013 Future of NIS Public Private Cooperation*, 2015, available at https://www.enisa.europa.eu/publications/ep3r-2009-2013.

[48] K. Iron, *The Governance of Network and Information Security In the European Union: The European Public-Private Partnership for Resilience (EP3R)*, in S. Gaycken, J. Krueger, B. Nickolay (a cura di), *The Secure Information Society: Ethical, Legal and Political Challenges*, Springer Publ., Berlin, 2021, pp. 83-116.

[49] JOIN/2013/01 final, Joint Communication … op. cit., p. 6.

[50] See The EC3 Advisory Groups – Law Enforcement and Private Sector Meetings to Discuss Lates at https://www.europol.europa.eu/media-press/newsroom/news/ec3-advisory-groups-%E2%80%93-law-enforcement-and-private-sector-meetings-to-discuss-latest-cybercrime-threats-and-challenges.

[51] See Europol and the European ATM Security Team reaffirm their partnership in combating payment crimes at https://www.europol.europa.eu/media-press/newsroom/news/europol-and-european-atm-security-team-reaffirm-their-partnership-in-combating-payment-crimes.

[52] Reference is made to agreements with Kaspersky, McAfee, Mnemonic, Microsoft, FireEye, the documentation of which can be found on the Europol website at https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-partners.

[53] R. Bossong, B. Wagner, *A typology of cybersecurity and Public-Private partnership in the context of the European union*, in O. Bures, H. Carrapico (edit by), *op. cit.*, p. 236.

Lastly, the European Defence Industrial Development Programme (EDIDP)[54] financed the development of the *European Cyber Situational Awareness Platform* (ECYSAP),[55] a Consortium of private actors aimed at laying innovative theoretical foundations, methods, research prototypes, and their integration to provide a European operational platform enabling real-time Cyber Situation Awareness with speed.[56]

In terms of integrated European security, as gleaned from official documents, it is important to note that the project's purpose is to develop a Cyber Situation Awareness (CSA) system «for National/European security purposes and military expeditionary operations will be developed, which shall become a real time defensive system capable of cyber response, automated and deployable in the same area of operations (National/European) interconnected between envisaged and identified intelligent nodes».[57]

5. The progressive Europeanization of information cooperation tools: Security Operations Centers (SOCs), vulnerability registers, exchange standards, and cyber threat sharing platforms

Having identified the reporting entities in the previous paragraphs, it is now essential to specify which tools and processes, they use to contribute to the flow of cybersecurity information.

a) Security Operation Centres (SOCs)

At the core of the information-sharing process related to cyber threats are Security Operation Centers (SOCs), public or private security operational centres that, through continuous monitoring of the networks and systems of the organization they operate for, prevent cyber attacks from negatively impacting the functioning and economy of the organization by minimizing damage.[58] These centres are not only capable of detecting ongoing threats but also of extracting particularly useful information, both for investigative activities conducted by law enforcement (such as digital forensics) and for prevention activities, such as information-sharing mechanisms.

In particular, this information asset consists of technical vulnerabilities, i.e., weaknesses in the system or IT assets that criminals have exploited to compromise their confidentiality, availability, or integrity; exploits, i.e., code specifically designed to exploit a particular vulnerability and compromise it, or other types of information, such as the so-called indicators of compromise (IoC), a term that generally refers to the Internet Protocol (IP) address of the server possibly used to carry out the attack, the Domain Name System (DNS) domain name, or suspicious Uniform Resource Locator (URL) pointing to malicious content, and finally, the identifier of a malicious executable file or the text of the subject of a malicious email message.[59]

Given that these centres are currently mostly established within individual entities and industrial realities, both public and private, it is important to highlight the mentioned Cyber Solidarity Act. If the proposed Regulation comes into effect without amendments, the establishment of the European Cybersecurity Shield would introduce two significant innovations in national and European cybersecurity architectures. It is expected that the "Shield" will be composed of national SOCs, of a public nature, designated by each Member State (Art. 4), and "Cross-border SOCs", i.e., cross-border centres established by a consortium of at least three Member States represented by national SOCs (Hosting Consortium), committing to work together to coordinate their cyber detection and threat monitoring activities (Artt. 6–7).[60]

On this last point, it is specified that the Consortia will be established based on written agreements in which the members must also detail the requirements and principles for sharing «relevant information» among the participants (Art. 6). Moreover, the proposal encourages individual Consortia to enter into agreements with other Consortia.

a) Vulnerability and Weakness Registries

In the early days of computing, the first "lists" of vulnerabilities were in use, created and maintained by the early users of the Internet Society (mostly composed of engineers and computer experts at the time)[61] through the Request for Comments (RFC).[62] It was a tool of transparency that well expressed the self-regulation characterizing the Internet. It is interesting to note that later, with the increasing significance of cyber attacks for societies and the economy, many of these registries are now mostly developed and supervised by a combination of private and public entities, subject to government oversight.[63]

In the United States, the Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) are active[64]: Two indices that fall within the vulnerability disclosure, namely the sharing of information about software vulnerabilities and weaknesses to facilitate the mitigation of the negative effects of unwanted access by security experts. These are programs for aggregating and publishing computer vulnerabilities and weaknesses overseen by a

[54] Please refer to the EDIDP website at https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-industrial-development-programme-edidp_en. About the ECYSAP project, please see the European Commission, factsheet at https://ec.europa.eu/commission/presscorner/api/files/attachment/865731/EDIDP%20-%20ECYSAP.pdf.pdf.

[55] Please refer to the link on the official ECYSAP platform website, available at https://www.ecysap.eu/concept.html.

[56] Ibid.

[57] European Commission ECYSAP factsheet.

[58] On the definition of SOC, reference is made to the guidelines ENISA, *How to set up CSIRT and SOC. Good practice guide*, December 2020, available at https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc.

[59] Regarding this matter, please refer to the information sheet published by the National Cyber Security Centre (NCSC), *Factsheet on Indicators of Compromise (IoCs)*, 2017 available at https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-indicators-of-compromise.

[60] On the formation of the consortium, the proposed Regulation envisages that members of the hosting consortium enter into a written consortium agreement that establishes their internal provisions, detailing the requirements for sharing information among participants in a cross-border SOC and for sharing information.

[61] The Internet Society (ISOC) is an international organization under American law for the promotion of the use and access to the Internet, now populated by various local sections (so-called chapters) with the participation of many countries worldwide. For further information, please refer to its official website at https://www.internetsociety.org/.

[62] The Repaired Security Bugs in Multics was the first "list" of vulnerabilities published in 1973 by Jerome H. Saltzer with RFC No. 5. For further details, refer to https://web.mit.edu/saltzer/www/publications/rfc/csr-rfc-005.pdf. The Request for Comments (RFC) are «documents containing technical specifications and organizational notes for the Internet», as defined by the international body that produces them, the Internet Engineering Task Force (IETF). The IETF is responsible for standardizing the Internet and the technical standards that enable its operation, foremost among them being the Internet protocol suite (TCP/IP).

[63] Despite the scarcity of official documents on this point, from Wiki sources, it is learned that the first (and perhaps only) vulnerability database developed by an independent entity, thus free from controls by public authorities, was the Open Sourced Vulnerability Database (OSVDB). It was an initiative that started at the well-known computer enthusiast convention, Def Con, in 2002, and became operational with the first open-source database in 2004 (therefore also free from proprietary ties with software companies) with the support of the Open Security Foundation (OSF). However, on April 5, 2016, the database was closed. For more details refer at https://en.wikipedia.org/wiki/Open_Source_Vulnerability_Database.

[64] Please refer to the websites of Common Vulnerabilities and Exposures at https://cve.mitre.org/ and Common Weakness Enumeration at https://cwe.mitre.org/.

private non-profit entity, the MITRE Corporation,[65] With support from the Cybersecurity and Infrastructure Security Agency under the U.S. Department of Homeland Security. Additionally, the databases related to CVEs are synchronously published on another registry, the National Vulnerability Database (NVD), managed and established by the public agency National Institute of Standards and Technology (NIST) in 2005.[66]

It will be understood, therefore, how the geographical origin of such databases is a matter of significant interest to governments. This is evidenced by the fact that, in addition to the more common ones just mentioned, of U.S. origin, similar information ecosystems have also been established in other countries, such as Japan,[67] China[68] and Russia.[69]

On this point, it seems relevant to note that Recital 63 of Directive 2022/2555 provides that «[a]lthough similar vulnerability registries or databases exist [i.e. CVE e CWE], they are hosted and maintained by entities which are not established in the Union». With the NIS II Directive, the European Union has indeed promoted, for the first time, the establishment of a European Vulnerability Registry maintained by ENISA to ensure «would provide improved transparency regarding the publication process before the vulnerability is publicly disclosed, and resilience in the event of a disruption or an interruption of the provision of similar services».[70]

However, while on the one hand, the disclosure of vulnerabilities and weaknesses within coordinated and freely accessible public databases can certainly promote cybersecurity among professionals, on the other hand, it can also be an easily exploitable tool for criminals with a keen interest in leveraging them to compromise networks and computer systems. For this reason, the European legislator entrusted ENISA to «ensure the security and integrity of the European vulnerability database». Also, in the Recital n. 58, it is envisaged «strengthening the coordination» between the reporters and the manufacturers or suppliers of ICT goods and services from which such vulnerabilities were detected, to expedite communication. It is also specified that the recital explicitly refers (fixed reference) to the international standards ISO/IEC 30111 and ISO/IEC 29147 regarding the management and disclosure of vulnerabilities to third parties.

However, at the moment, this register has not yet been set up, and according to recent statements of the ENISAs' Chief Cybersecurity Officer, it is doubtful whether it will be established at all.[71]

a) **Cyber Information Sharing Platforms and Sharing Standards**

Generally, sharing information about cybersecurity threats and alarms occurs through cyber information sharing platforms, which can be proprietary or open source (such as Malware Information Sharing Platform - MISP),[72] these platforms enable the dissemination and enrichment of this informational heritage through specific language standards (more precisely, standards on data format[73]).

However, for quite some time, the security market has witnessed the gradual introduction of highly advanced platforms - the so-called Cyber Threat Intelligence (CTI) platforms - tools capable not only of extracting and sharing information related to cyber threats and security incidents but also of processing them through cross-referencing with other external sources that allow them to provide - precisely - threat intelligence information.[74]

Specifically, the CTI was defined as an activity aimed at collecting «evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard».[75]

The aggregation of sources that characterizes threat intelligence activities indeed provides a comprehensive overview of the so-called tactics, techniques, and procedures (TTPs), namely: high-level descriptions of behaviour (tactics); detailed descriptions of behaviour within the context of a tactic (techniques); detailed descriptions within the context of a technique (procedures). TTPs thus allow for describing the tendency of an actor to use a specific variant of malware, a sequence of operations, an attack tool, a delivery mechanism (such as a phishing attack), or an exploit.[76]

Therefore - to put it in criminological terms - CTI platforms allow for the reconstruction of the "signature" and "modus operandi" of malicious actors,[77] providing information not only of a technical nature, useful for enriching the information pools typical of information sharing but also complex and aggregated information useful for any investigative activities by professionals.

The recent interest of States in cybersecurity has led part of the doctrine to question the legal aspects of these platforms. For a long time, these tools have been applied in the private sector without

[65] As learned from the official website of the organization, MITRE was established in 1958 as a private non-profit corporation to provide engineering and technical consulting to the United States Air Force. The project was instrumental in creating the first federally funded research and development centre (FFRDC), sponsored by the Department of Defense. Please refer to https://www.mitre.org/who-we-are/our-story.

[66] The NIST is part of the U.S. Department of Commerce. For further details, please refer to https://www.nist.gov/about-nist.

[67] Japan Vulnerability Notes (JVN), see https://jvn.jp/en/.

[68] Chinese National Vulnerability Database (CNNVD), see https://www.cnvd.org.cn/.

[69] Data Security Threats Database (BDU), if there is not much publicly available information, except for some journalistic articles v. J. Leiden, *Russia's national vulnerability database is a bit like the Soviet Union – sparse and slow 7 comment bubble on white By design, though, not... er, general rubbishness*, The Register, 17 July 2018, available at https://www.theregister.com/2018/07/17/russia_vuln_database/.

[70] Recital 63, NIS II Directive. Art. 29 of the Directive, provides that among the «relevant cybersecurity information» include, in addition to technical vulnerabilities, information related to cyber threats, near incidents, procedures, indicators of compromise (IoC), adversary tactics, specific information about threat actors, cybersecurity alerts, and recommendations regarding the configuration of cybersecurity tools to detect cyber threats.

[71] A. Martin, *EU cyber agency will not create active vulnerability database, says chief cybersecurity officer*, The Record, 18 April 2024 available at https://therecord.media/enisa- will-not-create-vulnerability- database-cyber- resilience- act.

[72] see MISP website at https://www.misp-project.org/.

[73] The most commonly used data formats for the operation of these platforms are the STIX/TAXII, CyBOX, and OASIS standards. For further technical details on the functioning of sharing platforms, please refer to the mentioned NIST guide as noted in footnote 94.

[74] It is important to distinguish cyber threat intelligence from cyber intelligence as an autonomous branch of intelligence. Cyber intelligence consists of «a set of programmed and applied activities to identify, track, measure, and monitor information about digital threats, as well as data on the intentions and activities of adversarial entities». These activities are carried out using «cyber tools in cyberspace, i.e., through the network, and have a peculiarity, unlike other forms of intelligence, as complete reliance cannot be placed on electronic equipment» see U. Gori, L.S. Germani (edit by), I*nformation Warfare 2011. La sfida della cyber intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, Franco Angeli, Milano, 2012, pp. 16 ss.

[75] Please refer to the page "Introduction to CTI as a General Topic" on the FIRST website, available at https://www.first.org/global/sigs/cti/curriculum/cti-introduction.

[76] C. Johnson, L. Badger, D. Waltermire, J. Snyder, C. Skorupka, *Guide to Cyber Threat Information Sharing*, NIST Special Publication 800-150, 2016, available at https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf.

[77] R. Chiesa, S. Ciappi, *Profilo Hacker. La scienza del criminal profiling applicata al mondo dell'hacking*, Milano, Apogeo, 2007, pp. 10 ss.

proper regulation,[78] especially regarding the handling of information and the protection of personal data, which will be explored in the next paragraph.

For what concerns the specific regulation related to the legitimate use of these tools, it seems useful to refer to the provisions of the NIS II Directive, where Art. 29, para. 3, stipulates that Member States «shall facilitate the establishment of cybersecurity information-sharing arrangements […]» and «specify operational elements, including the use of dedicated ICT platforms and automation tools, content and conditions of the information-sharing arrangements». The eventual participation in such information-sharing circuits must also be notified to the competent authorities at the time of concluding these agreements, as well as their withdrawal from them (see 3).

The main obstacle in information exchange is the lack of common standards in communication. Although recent NIS regulations do not impose compliance with common requirements in this regard, it seems useful to refer to a "work in progress" study conducted by ENISA regarding information exchange between CSIRTs and law enforcement authorities. The study proposed a taxonomy to identify which information can be shared between the two and how this can be achieved from a technical and organizational perspective.[79]

6. Security in the handling of "sensitive and classified" State information contained in cybersecurity information

From the brief overview of reporting entities outlined earlier, it emerges that the European legislator intended to distinguish critical entities («essential» and «important») from those not falling into this category based on their importance to the sector in which they operate, the type of services they provide, and their size.[80]

It is important to clarify that the infrastructures operating in these sectors fall not only under the scope of European regulations but also under the respective national legislations of the Member States, which, in some cases, like Italy, have not only implemented the NIS Directive[81] but have also adopted autonomous national cyber security legislation.

The clarification is necessary because, while for the NIS II Directive the measures laid down therein are aimed at ensuring a high common level of European cyber-security «to improving the functioning of the internal market» (Art. 1), the Decree-law n. 105 of 21 September 2019, by which Italy established the Perimetro di Sicurezza Nazionale Cibernetica,[82] provides for measures aimed at ensuring the «protection of national security and national interest in cyberspace» (Art. 1, co. 1, lett. a).[83]

The deep connection between national security and critical infrastructure protection[84] leads to the conclusion that the circulation in the European space of cybersecurity information - consisting of what we can imagine as the "access keys" to critical computer networks and systems - can be severely hampered by limits dictated by sovereign State prerogatives, such as internal security, different from the broader "European security" profile.

Another limitation is certainly represented by the protection of the fundamental rights of individuals. The material disseminated could make it possible to identify individuals, like the Internet Protocol (IP), qualified as personal data by constant European case law, whether dynamic or static,[85] email address, the *Uniform Resource Locator* (URL),[86] domain names (DNS),[87] but also banking information such as IBAN, as well as the identifier provided for the use of social networks. In this case, the disciplinary framework on the protection of personal data applies in different ways, depending on the nature of the data controllers. Will find application Regulation 2016/679, as a general personal data protection regulation; the Directive 2016/680 (also known as the "Law Enforcement Directive" - LED) on the protection of individuals about the processing of personal data by competent authorities for prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties[88]; Regulation 2018/1725, which lays down the rules applicable to the processing of personal data by EU institutions, bodies, offices and agencies; and finally, Regulation (EU) 2016/794, which governs the processing of personal data by the European Union Agency for Law Enforcement Cooperation (Europol).[89]

A further consideration concerns the propagation of cyber incidents that can easily scale from an internal emergency of a single organisation to a national or transnational emergency. This is why the information assets that characterise cyber information sharing can be used by different actors, for different purposes, ranging from the interest of organisations in safeguarding their business, or of public administrations

[78] L. O. Nweke, S. Wolthusen, *Legal Issues Related to Cyber Threat Information Sharing Among Private Entities for Critical Infrastructure Protection*, 2020 12th International Conference on Cyber Conflict (CyCon), Estonia, 2020, 63-78, available at https://ccdcoe.org/uploads/2020/05/CyCon_2020_4_Nweke_Wolthusen.pdf.

[79] ENISA, *Information sharing and common taxonomies between CSIRTs and Law Enforcement*, 2016, available at https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement.

[80] Recital 15 NIS II Directive.

[81] Decree-law, 18 May 2018, n. 65, with which Italy has implemented the NIS Directive.

[82] Decree law n. 105 of 2019, converted with amendments by Law n. 133 of 18 November 2019, is the legislative act by which Italy established "Perimetro di Sicurezza Nazionale Cibernetica" (eng. Cyber National Security Perimeter) (PSNC). Briefly, it is an articulated programme, concretely implemented using a series of administrative regulations, whose objective is to raise the security levels of the networks, information systems and IT services «of public administrations, public and private entities and operators based in the national territory, on which depends the exercise of an essential function of the State, or the provision of service essential for the maintenance of civil, social or economic activities fundamental to the interests of the State, and from the malfunctioning, interruption, even partial, or improper use of which may result in prejudice to national security, the national cyber security perimeter is hereby established».

[83] Art. 1, co. 1, lett. a) Decree-Law n. 105 del 2019.

[84] E. Żaboklicka, *Critical infrastructure in the shaping of national security*, Security and Defence Quarterly, 2020, 70-81, available at https://securityanddefence.pl/Critical-infrastructure-in-the-shaping-of-national-security,118585,0,2.html; B. Valensise, *I settori strategici dopo la riforma*, in G. Della Cananea, L. Fiorentino (a cura di), *I "poteri speciali" del Governo nei settori strategici*, Editoriale Scientifica, Napoli, 2020, pp. 101 ss.

[85] Ex multis, refer to the well-known Breyer judgment, CJEU, C-582/14, 19 October 2016. Please also refer to Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, stating that «some sorts of IP addresses which under certain circumstances indeed do not allow identification of the user, for various technical and organizational reasons. One example could be the IP addresses attributed to a computer in an internet café, where no identification of the customers is requested» (p. 17).

[86] See M. Korse, *Personal Data in URLs*, in *privacywise*, 23 August 2017, available at https://www.privacy-wise.com/personal-data-in-urls/.

[87] The Internet Corporation for Assigned Names and Numbers (ICANN), which operates the Domain Name System (DNS), is also responsible for managing the WHOIS registry, a public database according to which anyone with a web domain must register not only their domain but also their names, addresses, e-mail addresses and telephone numbers. See S. Vaughan-Nichols, *DNS is about to get into a world of trouble with GDPR*, Zdnet, 18 April 2018, available at https://www.zdnet.com/home-and-office/networking/dns-is-about-to-get-into-a-world-of-trouble-with-gdpr/.

[88] See in general E. Kosta, F. Boehm (edit by), *The EU Law Enforcement Directive (LED). A Commentary*, Oxford University Press, 2023.

[89] For a discussion of the application of data protection disciplines with regard to cyber infromation sharing processes be granted reference to F. Serini, *Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche. Verso una definizione di cybersicurezza integrata?*, MediaLaws Review, n. 3, 2023, available at https://www.medialaws.eu/wp-content/uploads/2024/01/3-23-Serini.pdf.

in the efficient and continuous delivery of services, to the defence of national security by governments and European security.

This section will therefore attempt to analyse the differentiated treatment regime of cybersecurity information given the fact: (a) that this information may be used for the protection of the internal security of Member States and therefore could be classified or could be qualified as "sensitive", effectively limiting its circulation; (b) that this information could be a point of failure of national critical systems as relevant institutions and critical infrastructures.

a) **The dissemination of "sensitive and classified" cybersecurity information and the limits to its circulation**

In the 2020 Strategy mentioned above Paper, the Commission noted that «the interoperability of classified information systems remains limited, preventing a seamless transfer of information between the different entities» thus recognising the need for an interinstitutional approach to the handling of classified information at the European level, including through the identification of «[a] baseline should also be established to simplify procedures with Member States».[90]

As can be deduced from the proposal for the EU Cyber Solidarity Act Regulation, these procedures are still in the implementation phase, and above all, a suitable basis of legitimacy has yet to be identified. The subject is extremely sensitive, since information cooperation, which is part of the broader concept of collective security,[91] clashes with the limitations imposed for internal security reasons by the Member States.

In this regard, it seems useful to recall the content of Art. 346, lett. a) TFEU. This provision is one of the provisions authorising a derogation from the application of the rules of the TFEU by non-economic reasons (safeguard clause), authorised in the name of national security and defence requirements to achieve a delicate balance between the aforementioned internal needs of States and the fundamental objectives of the internal market.

In particular, under the hypothesis of paragraph 1, lett. a), the Member States are allowed to refuse to supply information to any European institution whose disclosure is considered by them to be «contrary to the essential interests of its security»,[92] provided that such a restrictive measure is deemed necessary and never for economic reasons.

The doctrine has variously debated the interpretation of the provision between restrictive and extensive approaches.[93] According to the Commission, the provision «goes beyond defence, aiming in general at protecting information which Member States cannot disclose to anyone without undermining their essential security interests».[94]

Therefore, the derogation in question exempts States from the broader obligation arising from the principle of loyal cooperation under Article 4(3) TEU, which requires States to provide the EU institutions (including the Court of Justice) or other Member States with information requested from them to keep secret that which concerns their security.

The application of Article 346 TFEU in the context of cyber information sharing is reflected in the EU Cyber Solidarity Act, where Recital 23 stipulates that the exchange of information must take place within the limits of the («without prejudice»), and also that such dissemination «should be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of such information should preserve the confidentiality of the information and protect the security and commercial interests of the entities concerned, in full respect of trade and business secrets».

In this regard, Recital 9 of the NIS II Directive states that the regulation of such trafficking should take place in compliance with the «Union or national rules for the protection of classified information, non-disclosure agreements, and informal non-disclosure agreements such as the traffic light protocol should be taken into account in that context» (we will return to the latter shortly), and in the following Recital 118 it is stipulated that «ENISA should have the infrastructure, procedures and rules in place to handle sensitive and classified information following the applicable security rules for protecting EU classified information».

The exchange and protection of "sensitive and classified" information in the European context is an evolving discipline that has advanced over time through agreements and decisions between the European Union and individual States, including non-EU members.[95]

Without going into detail, briefly, the parties agree to develop cooperation on the security and sharing of classified information by adhering to certain common prerogatives: each party shall protect classified information provided by, or exchanged with, the other at a level at least equivalent to that provided by the providing party; all persons having access to classified information shall have an appropriate security clearance, based on loyalty, trustworthiness and reliability; restrictions may also be established on how classified information may be used and disclosed, and on access to it.

On this point, it is useful to point out that according to Art. 2 of Decision 2013/488/EU, «EU classified information» (EUCI) is intended «any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States».[96]

However, as pointed out in doctrine, the clause in the aforementioned Article 346(a) TFEU applies only to Member States and not also to undertakings.[97]

[90] JOIN/2020/18 final.

[91] World Economic Forum, *Cyber Information Sharing: Building Collective Security. Insight Report*, October 2020, available at https://www3.weforum.org/docs/WEF_Cyber_Information_Sharing_2020.pdf.

[92] This is a safeguard clause provided for by the Treaty that applies only in the hypotheses covered by the provision. Introduced to protect state secrecy concerning the national security of member states, this Article represents a derogation from Artt. 4 (3) TEU and 337 TFEU, the former dedicated to the obligation to provide information to the European institutions by the principle of loyal cooperation, the latter giving the European Commission the power to gather all necessary information and carry out the appropriate checks for the performance of its tasks.

[93] On the restrictive approach see P. Gori, *Art. 223*, in R. Monaco, R. Quadri, A. Trabucchi (edit. by), *Commentario CEE*, GiuffrèMilano, 1995, pp. 1626 ss.; for another orientation, of extensive interpretation see R. Smit, P. Herzog, *Article 223*, in P. Herzog, C. Campbell, G. Zagel (edit. by), *The Law of the European Union is the completely updated and revised edition of their Law of the European Community: A Commentary on the EC Treaty*, Lexis nexis, New York, vol. 5, 2018.

[94] COM(2006)779 7 December 2006 on the application of Article 296 of the Treaty in the field of defence procurement, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0779.

[95] For an overview see the Eur-Lex website available at https://eur-lex.europa.eu/EN/legal-content/summary/agreements-on-the-security-of-classified-information.html. V. anche E. De Capitani, *Unione europea e segreto di Stato*, Astrid-online, 2010.

[96] Top Secret: information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the EU or of one or more EU countries; 2. EU Confidential: information and material the unauthorised disclosure of which could harm the essential interests of the EU or one or more EU countries; 4. EU Restricted: information and material the unauthorised disclosure of which could be disadvantageous to the interests of the EU or one or more EU countries.

[97] F. Sciaudone, *Art. 346 TFUE*, in A. Tizzano (a cura di), *Trattati dell'Unione europea, Le fonti del diritto italiano*, II ed., Milano, Giuffré, 2014, pp. 2515 ss.

A principle that is also reflected in the context of cybersecurity information exchanges, given the content of Recital 10 of the aforementioned NIS II Directive, which, after highlighting the connection between critical infrastructures active in the nuclear power generation sector and national security, provides that «a Member State should be able to exercise its responsibility for safeguarding national security with respect to those activities, including activities within the nuclear value chain, in accordance with the Treaties».

It therefore reaffirms the exclusive competence of States to take the necessary measures to ensure the protection of essential national security interests and safeguard public order and public safety, by promoting the use of voluntary cybersecurity information-sharing agreements with critical actors «in respect of the potentially sensitive nature of the information shared» (Art. 29, para. 2).

Among the legal bases mentioned in the NIS II are also the «informal non-disclosure agreements such as the traffic light protocol»,[98] or TLP. This is an international standard developed by FIRST (Forum of Incident Response and Security Teams)[99] to facilitate the sharing of potentially sensitive information and more effective collaboration.

In cases where the exchange of information is deemed contrary «to the essential interests of its security»[100] and thus States can refuse to provide information to any organisation in the Union, at a general level, cybersecurity information traffic is usually handled by the aforementioned TLP standard, consisting of «a set of four labels used to indicate the sharing boundaries to be applied by the recipients».[101] Specifically, these labels are represented by four colours: red, represents the highest restriction and indicates information that cannot be disclosed to the public but only to individual recipients because it could compromise the confidentiality of individuals, secrets, reputation or the organisation's business; yellow, indicates information whose disclosure is restricted to the organisation and its clients with the caveat that its circulation should be subject to special safeguards when its transfer could compromise the confidentiality of individuals, secrets, reputation or the organisation's business; green, indicates information that can be disseminated among the members of the information circuit to which the CTI platform belongs, usually information useful for raising awareness within their community. On the other hand, there are no restrictions for information that carries little or no risk of misuse, under the applicable rules and procedures for public disclosure.

a) **The "active exploited vulnerabilities" of ICT products**

The proposal Regulation on horizontal cybersecurity requirements for products with digital elements, the so-called *Cyber Resilience Act* (CRA), has introduced the concept of «actively exploited vulnerability», defined as «a vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without permission of the system owner» (Art. 3 n. 42).

This cybersecurity information is particularly sensitive because it represents a vulnerability that is difficult to remediate within the twenty-four hours required for notification, and therefore poses a potential danger if learnt by malicious actors who may exploit it again.[102] Dissemination of this kind of information has been part of a debate during the trialogue[103] between the European Parliament, intended to entrust ENISA as the only recipient, and the representations of the Member States' governments, fearing that such vulnerabilities might pose risks to national security and interests, proposed to transfer this function to the national CSIRTs.[104]

The version accepted by the Parliament[105] indicated in Art. 14, par. 1, that the manufacturer shall notify these vulnerabilities contained in the product with digital elements «simultaneously to the CSIRT designated as coordinator, […] and to ENISA» via the single reporting platform managed and maintained by ENISA.

However, Art. 16 where disciplined the establishment of this single reporting platform, states at par. 2 that «in exceptional circumstances and, in particular, upon request by the manufacturer and in light of the level of sensitivity of the notified information […], the dissemination of the notification may be delayed based on justified cybersecurity related grounds for a period of time that is strictly necessary, including where a vulnerability is subject to a coordinated vulnerability disclosure procedure […]» and «[w]here a CSIRT decides to withhold a notification, it shall immediately inform ENISA about the decision and provide both a justification for withholding the notification as well as an indication of when it will disseminate the notification in accordance with the dissemination procedure laid down […]».

Also, only in particularly exceptional circumstances, where the manufacturer indicates in the notification that a) the vulnerability has been exploited in no other Member State than the one of the CSIRT designated as coordinator; b) that any immediate further dissemination of the notified vulnerability would likely result in the supply of information the disclosure of which would be contrary to the essential interests of that Member State; c) or that the notified vulnerability poses an imminent high cybersecurity risk stemming from the further dissemination, are made available simultaneously to ENISA «only the information that a notification was made by the manufacturer, the general information about the product, the information on the general nature of the exploit and the information that security related grounds were raised» until the full notification is disseminated to the CSIRTs concerned and ENISA. In this case, the notification does not contain information that may be of interest to the internal security of the Member States.

But, where ENISA considers that there is a systemic risk affecting security in the internal market, it shall recommend to the recipient CSIRT that it disseminate the full notification to the other CSIRTs designated as coordinators and to ENISA itself.

[98] Recital 9, and Art. 10, para. 7, NIS II Directive.

[99] FIRST is a global forum bringing together computer security incident response teams, created in the United States in 1989 following the establishment of the first CERT. For more details, please refer to https://www.first.org/tlp/.

[100] Art. 346, let. a), TFUE.

[101] The definition was taken from the FIRST website.

[102] On this point, see the open letter of European Digital Rights (EDRi), "Make vulnerability disclosure in the Cyber Resilience Act more secure, not less" available at https://edri.org/our-work/open-letter-make-vulnerability-disclosure-in-the-cyber-resilience-act-more-secure-not-less/.

[103] For the topics discussed by the various trilogues, please refer to the articles in Euractiv signed by Luca Bertuzzi, specifically see L. Bertuzzi, *EU Commission pitches double reporting of open security loopholes in cybersecurity law*, Euractiv, 15 November 2023, available at https://www.euractiv.com/section/cybersecurity/news/eu-commission-pitches-double-reporting-of-open-security-loopholes-in-cybersecurity-law/; ID, *EU policymakers prepare to close on cybersecurity law for connected devices*, Euractiv, 30 November 2023, available at https://www.euractiv.com/section/cybersecurity/news/eu-policymakers-prepare-to-close-on-cybersecurity-law-for-connected-devices/; ID, *EU institutions finalise agreement on cybersecurity law for connected products*, Euractiv, 5 December 2023, available at https://www.euractiv.com/section/cybersecurity/news/eu-institutions-finalise-agreement-on-cybersecurity-law-for-connected-products/.

[104] The European Council's proposals on the CRA can be found at https://www.consilium.europa.eu/en/press/press-releases/2023/07/19/cyber-resilience-act-member-states-agree-common-position-on-security-requirements-for-digital-products/.

[105] European Parliament legislative resolution of 12 March 2024 (COM(2022) 0454 – C9-0308/2022 – 2022/0272(COD)) available at https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html.

7. Concluding considerations

Situational awareness processes are an optimal solution for pervasive and easily scalable threats such as cyber attacks, especially during periods of instability in international relations. However, this study has highlighted the gap between the political project, repeatedly raised by European institutions, of creating a situational awareness process in cybersecurity within the EU and the related legal implications.

Drawing inspiration from President von der Leyen's words in the 2021 State of the Union address, we have developed the concept of Collective Cyber Situational Awareness (CCSA), as a Cyber Situational Awareness (CSA) process common to all Member States.

Considering that such a process was supposed to be implemented in a political union of States like the EU, we hypothesized that many of the difficulties characterizing the implementation of CSA processes — first and foremost the lack of trust among participants — could find an easy solution through legislative harmonization in the field of cybersecurity, the adoption of common techniques, and the allocation of resources.

The study, however, revealed that although ad hoc institutions have been created at the organizational level, partnerships involving law enforcement and various actors involved in cybersecurity policies have been promoted, legislation favouring information exchange among all involved actors (both public and private) has been implemented, and specific technical remedies have been developed at the European level, the creation of a common decision-making process in the Union is a difficult project to realize.

The reason can be attributed to the fact that the European security system has never found full communitarization. Security in the European dimension appears on one hand as a common objective when the Union acts to protect the internal security of European citizens, but on the other becomes a limiting factor to the founding freedoms of the Union — including the free flow of information — when invoked by Member States.[106] See the clauses in the Treaties protecting "national security" or "public order and security" that suspend the Treaties' application in favour of Member State prerogatives.

Regarding the circulation of cybersecurity information among Member States, as noted in our analysis, this can be strongly limited or interrupted for reasons of internal security. Information collected following a cyber attack can indeed contain not only technical indications but also information that can be classified as sensitive or classified for the Member State.

This is the case with the "actively exploited vulnerabilities" governed by the proposed Cyber Resilience Act. However, this Act provides that although such vulnerabilities may be relevant to a State's internal security and their dissemination may pose risks, if ENISA considers that there is a systemic risk affecting the security of the internal market, it will recommend that the recipient national CSIRT disseminate the full notification to the other CSIRTs designated as coordinators and to ENISA itself.

The entry into force of this regulation will allow us to verify whether these provisions will find practical application and effectiveness to facilitate cyber information sharing processes and thus develop a possible CCSA. In the meantime, given the current difficulties in establishing a common decision-making process, we believe that a possible solution could be to promote greater situational awareness within individual Member States (bottom-up approach)[107] e.g. with a «customizable information-sharing»[108] process that could minimize[109] the cybersecurity information to be disseminated, acting as a filter that would, on the one hand, allow States to have control over the information to be disseminated and, on the other hand, feed the dissemination of that information if it is not deemed by the political authority to be of relevance to the State's internal security. Beyond theoretical solutions, however, there remains a need for ever-increasing cooperation between the Member States, in order to progressively develop better horizontal cooperation in cybersecurity processes at European level, based on mutual trust.

Declaration of competing interest

The author declare that he have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgements

I would like to deeply thank Professors Irene Kamara and Marco Bassini for the opportunity and their precious suggestions.

[106] see S. Peers, *National Security and European Law*, in *Yearbook of European Law*, Volume 16, Issue 1, 1996, Pages 363–404, available at https://academic.oup.com/yel/article-abstract/16/1/363/1718740.

[107] The city of Rome in 2017 was selected as a testing ground for a cyber situational awareness program (CS Aware) through an agreement with the Municipality and the European Commission under the Horizon 2020 program (Call: H2020-DS −2016 −2017). The main objective of this project was to to equip local public administrations with a toolset allowing them to gain a better picture of vulnerabilities and threats or infiltrations of their ICT systems. See T. Schaberreiter, J. Roning, Gerald Quirchmayr, V. Kupfersberger, C. Wills, M. Bregonzio, A. Koumpis, J. E. Sales, L. Vasiliu, K. Gammelgaard, A. Papanikolaou, K. Rantos, Arnolt Spyros, *A Cybersecurity Situational Awareness and Information-sharing Solution for Local Public Administrations Based on Advanced Big Data Analysis: The CS-AWARE Project*, Challenges in Cybersecurity and Privacy - the European Research Landscape, 2019, pp. 149-180.

[108] R. Baldoni, *Charting digital sovereignity: a survival playbook. How to assess and to improve the level of digital sovereignty of a country*, Independently published, Torrazza Piemonte, 2024, pp. 138 ss. The Author theorises the structure of "fusion cells" as an institutional architecture that would allow specific national security threats to be dealt with by preventing, detecting and mitigating their effects through a dynamic system of information exchange (input and output) between them, where «the method of structuring information exchange is determined by political authority or the leaders of the involved cells» (p. 141).

[109] Refer to a kind of "data minimisation" principle, well know in Art. 5, para. 1, let. c, Reg. UE 2016/679 (GDPR).