PEACE & SECURITY – PAIX ET SÉCURITÉ INTERNATIONALES
EuroMediterranean Journal of International Law and International Relations
Issue 12, January-December 2024 | ISSN 2341-0868
DOI http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

Citation: SEATZU, F. & CARRILLO SANTARELLI, N. , "On the law, work and functioning of the EU agency for cybersecurity", *Peace & Security – Paix et Sécurité Internationales*, No 12, 2024.

Received: 18 March 2024.
Accepted: 7 July 2024.

ON THE LAW, WORK AND FUNCTIONING OF THE EU AGENCY FOR CYBERSECURITY

Francesco SEATZU[1]
Nicolás CARRILLO SANTARELLI[2]

ABSTRACT: The EU Cyber Security Agency (carrying the acronym ENISA from its original name) is the main agency for the EU's cyber security programme. ENISA was initially created as an advisory body rather than as a monitoring agency and its unique approach reflects the EU's shift towards a more regulatory approach to cyber security problem-solving. This study explores the role of ENISA in governance and presents the complex concept of observational memory "observation" from a critical perspective. ENISA's monitoring approach has allowed it to become a new form of management, with a model reminiscent of vision. This perspective has had a significant impact on the development of the EU cyber security regime and has challenged the traditional understanding of ENISA as an advisory body on cyber security issues. As the Agency debates the balance between government and regulation, it continues to re-evaluate its role in the evolving cyber security landscape, forcing reflection on its success and events that shed light on cyber security issues.

KEYWORDS: The EU Agency for Cybersecurity; EU Agencies; Cybersecurity Governance; Monitoring Strategy; Surveillance.

SOBRE LA LEGISLACIÓN, LA LABOR Y EL FUNCIONAMIENTO DE LA AGENCIA DE LA UE PARA LA CIBERSEGURIDAD

RESUMEN: La Agencia de Ciberseguridad de la UE (conocida por su acrónimo en inglés, ENISA) es la principal agencia del programa de ciberseguridad de la Unión Europea (en adelante, UE). ENISA se creó inicialmente como un organismo asesor más que como una agencia de supervisión y su enfoque único refleja el cambio de la UE hacia un enfoque más regulatorio para la resolución de

[1] Full Professor of Public International Law, University of Cagliari (Italy). This article is part of the research project, Grant PID2020-112577RB-100, funded by MCN/AEI/10.13039/501199911033.

[2] Postdoctoral Researcher, University of Cagliari (Italy)

problemas de ciberseguridad. Este estudio explora el papel de ENISA en la gobernanza y presenta el concepto complejo de la memoria observacional "observación" desde una perspectiva crítica. El enfoque de supervisión de la ENISA le ha permitido convertirse en un nuevo modelo de gestión que recuerda a la visión. Esta perspectiva ha tenido un impacto significativo en el desarrollo del régimen de ciberseguridad de la UE y ha desafiado la comprensión tradicional de ENISA como un organismo asesor sobre cuestiones de ciberseguridad. Mientras la Agencia debate el equilibrio entre gobierno y regulación, continúa reevaluando su papel en el cambiante panorama de la ciberseguridad, lo que obliga a reflexionar sobre su éxito y los eventos que arrojan luz sobre las cuestiones de ciberseguridad.

PALABRAS CLAVE: Agencia de Ciberseguridad de la UE; Agencias de la UE; Gobernanza de la Ciberseguridad; Estrategia de Monitoreo; Vigilancia.

SUR LA LÉGISLATION, LE TRAVAIL ET LE FONCTIONNEMENT DE L'AGENCE DE L'UE POUR LA CYBERSÉCURITÉ

RÉSUMÉ: L'Agence européenne de cybersécurité (connue sous son acronyme en anglais, ENISA) est l'agence chef de file du programme de cybersécurité de l'UE. L'ENISA a été initialement créée comme un organisme consultatif plutôt que comme une agence de surveillance et son approche unique reflète l'évolution de l'UE vers une approche plus réglementaire pour résoudre les problèmes de cybersécurité. Cette étude explore le rôle de l'ENISA dans la gouvernance et présente le concept complexe d'"observation" de la mémoire observationnelle dans une perspective critique. L'approche de surveillance de l'ENISA lui a permis de devenir un nouveau modèle de gestion qui rappelle la vision. Cette perspective a eu un impact significatif sur le développement du régime de cybersécurité de l'UE et a remis en question la conception traditionnelle de l'ENISA en tant qu'organisme consultatif sur les questions de cybersécurité. Alors que l'Agence débat de l'équilibre entre gouvernance et réglementation, elle continue de réévaluer son rôle dans le paysage changeant de la cybersécurité, obligeant à réfléchir à son succès et aux événements qui mettent en lumière les enjeux de cybersécurité.

MOTS-CLÉS: Agence européenne de cybersécurité; Agences de l'UE; Gouvernance de la cybersécurité; Stratégie de surveillance; Surveillance.

I. INTRODUCTION

On 13 March 2004, the European Union (EU) created a key institution to address the evolution of cyber security: the European Union Cybersecurity Agency, known as ENISA. Departing from traditional methods of tackling cyber security issues, ENISA functions within a changing paradigm marked by the use of governance language, setting it apart from typical EU agencies[3].

[3] On the EU agencies, see *ex multis* Chamon, M., *EU Agencies: Legal and Political Limits to the Transformation of the EU Administration*, Oxford, 2016; Tovo, C., *Le agenzie decentrate dell'Unione europea,* Naples, 2016; Görisch, C., "Die Agenturen der Europäischen Union"*, JURA-Juristische Ausbildung*, Vol. 38, No. 4, 2012, p. 10 ff; Vos, E., "Reforming the European Commission: What role to play for EU agencies?", *Common Market Law Review*, Vol. 37, No. 5, 2000, pp. 1113-1134; Chamon, M., "EU Agencies: Does the Meroni Doctrine Make Sense?", *Maastrich Journal of European and Comparative Law,* Vol. 17, No. 3, 2010, p. 281 ff.

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

The primary objective of ENISA, outlined in Regulation (EC) No. 460/2004, is to offer guidance to the European Parliament, the European Commission, the European institutions, or the designated competent national body chosen by the Member States. Consequently, ENISA is distinguished by its "advisory mandate". These features categorize the Agency as a "novel governance instrument", mirroring the EU's shift towards inventive governance strategies. In this context, "governance" indicates a departure from the "social practices" outlined in the EU Commission's Governance White Paper[4]. The traditional approach hinges on the Commission's exclusive authority for legislative initiative, alongside the legislative powers vested in both the Council of Ministers and the European Parliament. This involves mechanisms specifically designed for legislating at the EU level. ENISA certainly conforms to this framework, as it is not explicitly outlined in the hierarchical institutional structure of the EU treaties. It demonstrates features such as decentralization, multi-level integration, power-sharing, deliberation, participation, flexibility, and knowledge creation. These characteristics collectively encapsulate the essence of "governance" within the context of the European Union[5].

Nevertheless, in addition to the Agency's advisory role, several alternative missions were contemplated both prior to and notably after the enactment of Regulation No. 460/2004. During the initial phases of proposal and negotiation, monitoring was considered a fundamental responsibility for the new agency[6]. However, a few years after the adoption of Regulation No. 460/2004, specifically in the latter months of 2007, there was a reduction in emphasis on the monitoring role[7]. ENISA, it appears, was intentionally not designed as a warning system that would signal alerts in the face of potential

[4] On the EU Commission White Paper on Governance, see Armstrong, K.A., "Rediscovering civil society: the European Union and the White Paper on Governance"*, European Law Journal,* Vol. 8, No. 1, 2012, pp. 102-132.

[5] For an exploration of the essence of governance within the EU context, see e.g. Maas, W., "European governance of citizenship and nationality", *Journal of Contemporary European Research,* Vol. 12, No. 1, 2016, p. 15 ff.

[6] COM (2003) 63.

[7] See also Kopchev, V., "The European Union Moves Ahead on Cybersecurity Research Through Enhanced Cooperation and Coordination"*, Information & Security: An International Journal*, Vol. 43, No. 3, 2019, pp. 67-81, emphasising that on 13 September 2017, the Commission adopted a comprehensive cyber security package incorporating a series of initiatives aimed at further enhancing EU cyber-resilience, deterrence, and defense.

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

cyber-attacks. ENISA, it seems, was intentionally crafted without the primary purpose of serving as a warning system to signal alerts in the event of potential cyber-attacks.

This article suggests that ENISA's role associated with governance essentially reveals a type of monitoring more accurately interpreted as surveillance. Surveillance is critically analysed in this context. Surveillance implies power relations, signifying processes that unveil the dynamics of power in both disciplinary and governmental aspects. This is noteworthy as it illustrates that ENISA operates through processes that facilitate a mode of governance characterized by discipline. These processes encompass providing advice and expertise, relying on networks of experts, and gathering statistical data.

Interpretation of ENISA's current role and work is interesting, especially as the EU's mission has changed from state-centred to governance-oriented[8]. Therefore, ENISA is concealing its supervisory function under the umbrella of governance, portraying itself as a "beacon on cybersecurity" and a model of apolitical progress[9]. The critique presented in this work exposes and questions these assumptions.

Emphasising ENISA's monitoring role reveals the power dynamics within the Agency's processes is not inherently negative. Disciplinary power is generative in crafting identities, shaping ENISA as the EU's cyber security institution, defining the EU as a cyber security actor and moulding the identities of the subjects engaged in the cyber security discourse, including EU citizens, Member States and other actors collaborating with ENISA, such as national and international NGOs. Certainly, it is this constructive facet of power that situates ENISA as a powerful new governance tool: ENISA governs by monitoring the EU space, amassing statistics and data on its compliance with and respect for cyber security rules and standards, and propagating a discourse centred on cyber security.

It governs to the extent that this discourse establishes the norm of a safe and secure Europe where fundamental rights and freedoms are safeguarded, portraying the EU as a cyber security organisation —strengthened by the presence of a cyber security agency— and shaping the perception of the preferred subjects in this society, such as the "individuals and entities resilient against cyber security attacks", and the "cyber security resilient Member State"[10].

It is essential to recognise the disciplinary and governing capabilities of organisations like ENISA tasked with safeguarding and advancing best practices, such as cyber security. This awareness enables us to resist forms of government and discipline, rather than passively accepting them under the guise of apolitical progress. Additionally, it is crucial to understand how this turns cyber security into a discourse employed for discipline and governance rather than solely for emancipation. This awareness empowers us to question and resist the level of government in the name of cyber security.

Moreover, the preceding considerations should make one explore the risks that a discourse focused exclusively on security considerations can entail in terms of generating domestic atmospheres in which fundamental rights are ignored in the name of effectiveness during the pursuit of that goal, and on the regression or absence of guarantees to contest the design and implementation of security monitoring and reporting.

We will therefore provide suggestions on how ENISA can consider the impact of its assessments and include references to human rights guarantees in ways that will promote rights-respectful and -promoting cybersecurity practices.

II. CYBERSECURITY MONITORING AND ENISA

The connection between ENISA and "monitoring" likely originates from its initial title as the "European Network and Information Security Agency", underscoring its emphasis on networks and security matters. The EU Commission's initial proposal in 2004 sought to establish a supervisory organisation with a focus on addressing information security concerns[11].

[8] See Hout, W., "Governance and Development: changing EU policies", in Hout, W. (ed.), *EU Strategies on Governance Reform: Between Development and State-building,* Sweet and Maxwell, London, 2012, pp. 1-16.

[9] See ENISA's official webpage for more detailed information.

[10] See also Backman, S., "Risk vs. threat-based cybersecurity: the case of the EU", *European Security*, Vol. 32, No. 1, 2023, p. 85 ff; Segura, A., *El desafío de la ciberseguridad global*, Tirant lo Blanch, Valencia, 2023; Bendiek, A., Bossong, R. and Schultze, M., *The EU's revised cybersecurity strategy: half-hearted progress on far-reaching challenges*, Deutsches Institut für Internationale Politik und Sicherheit, Berlin, 2017.

[11] COM (2003) 63.

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

Although the Commission's proposal called for the establishment of such a body, there was not enough detail on the necessity of a legal body that will provide or collect information.

Following the recommendations of the European Commission, the Council of the European Union recognised the lack of such a body and requested the creation of a supervisory body as part of the overall preparations for EU action to promote cybersecurity[12].

Recognising the importance of collecting and verifying cyber security information, the European Council agreed in 2007 to extend ENISA's mandate to establish an EU cybersecurity certification framework[13]. The deliberate omission of the word "monitoring" from ENISA's name appears to be intentional.

Before 2004, the European Commission had worked to address the need for regulatory bodies in the field of cybersecurity[14]. In doing so, it was inspired (though not explicitly) by the OECD Guidelines for the Security of Information Systems and Networks adopted in 2002[15]. These guidelines emphasised the importance of implementing common rules and principles for information security, providing a foundation that supports continuous initiatives at the European level. Additionally, the EU Commission was motivated by the acknowledgment of the necessity for "systematic and regular observation" to assess the adherence of Community and, now, Union institutions, bodies, offices and agencies to cyber security rules and standards[16]. This initiative also aimed to actively foster awareness of cyber security at various levels.

[12] Amplius, see e,g, Markopoulou, D. and Papakonstantinou, V., "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation", *Computer Law & Security Review,* Vol. 35, No. 6, 2019, p. 5 ff.

[13] See also Mitrakas, A., "The emerging EU framework on cybersecurity certification", *Datenschutz und Datensicherheit – DuD,* Vol. 42, No. 2, 2018, p. 411 ff.

[14] For further references, see Brandão, A. and Camisão, P., "Playing the Market Card: The Commission's Strategy to Shape EU Cybersecurity Policy", *JCMS: Journal of Common Market*, Vol. 60, No. 5, 2022, pp. 1335-1355.

[15] The text of the Guidelines for the Security of Information Systems and Networks is available at: https://www.enisa.europa.eu/topics/risk-management/current-risk/laws-regulation/corporate-governance/oecd-guidelines.

[16] See Brandão, A.P. and Camisão, I., *op. cit.* p. 1336.

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

The EU Commission also acknowledged the necessity for systematic and regular observation of how Member States both respect and promote cyber security rules and standards in practice when implementing EU law and policies[17]. The concept of "monitoring in a legal sense" was understood as the legal oversight of the proper application of EC/EU law, and it was considered a function reserved exclusively for the European Commission[18]. Such monitoring couldn't be delegated to a community agency to maintain the institutional balance of power. Instead, ENISA would carry out observatory monitoring. However, the emphasis on "systematic and regular observation" of the European Union and the Member States, particularly when implementing EU law, did not make it into the final text of the regulation.

ENISA was originally established as a "watchdog", tasked with overseeing cyber security standards and policies through monitoring[19]. However, the actual landscape of surveillance law differs from the perception of the new EU institutions. Genuine and more stringent oversight of cyber security standards and policies involves the input of independent experts, often recognised with one or more opinions on legal or judicial supremacy. This allows assessing government or other organizations' compliance with important procedures affecting the prevention of cyber-attacks[20]. A prime example of this is international human rights monitoring, where normative assessments are carried out by treaty-based human rights courts or expert bodies[21].

[17] *Ibidem*.

[18] *Ibidem*.

[19] See Schneider, V. and Hyner, D., "Security in Cyberspace: Governance by Transnational Policy Networks", in Koenig-Archibugi, M. and Zürn, M. (eds.), *New Modes of Governance in the Global System Exploring Publicness, Delegation and Inclusiveness*, Sweet and Maxwell, London, 2006, pp. 154-176.

[20] See also Article 3, para. 1 of the Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA, providing that: "ENISA shall carry out the tasks assigned to it under this Regulation for the purpose of achieving a high common level of cybersecurity across the Union, including by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. ENISA shall act as a reference point for advice and expertise on cybersecurity for Union institutions, bodies, offices and agencies as well as for other relevant Union stakeholders".

[21] See e.g. Wille, P.F., "The United Nations' Human Rights Machinery: Developments and Challenges", in Alfredsson, G., Grimheden, J., Ramcharan, B. and Zayas, A. (eds.), *International*

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

The scope of this mandate goes beyond mere information collection. The conceptual model for ENISA more closely resembles an "observatory" than an international expert body engaged in normative assessments, thereby reinforcing the assertion that ENISA would not engage in genuine, legal, normative monitoring. While one could argue that ENISA's proposed role in collecting and analysing data diminishes the authentic monitoring function, we dissent from this viewpoint. Instead, we contend that analysis and data collection empower ENISA to conduct surveillance. Operating as an observatory, ENISA functions as a surveillance mechanism, embodying a model for the exercise of disciplinary power.

ENISA's Regulation (EU) 2019/881 does allude to monitoring, but it neither provides a clear definition of the term nor attempts to elaborate on it. Specifically, paragraph 57 of the Preamble describes the Management Board as the body oriented to ensure that the Agency carries out its tasks under conditions that enable it to serve in accordance with this Regulation[22]. Furthermore, Article 59 to the Preamble mentions that the *ad hoc* Working Groups should enable the Agency to: "address specific matters, in particular matters of a scientific, technical, legal or socioeconomic nature".

The current institutional discourse underscores that ENISA's role is not strictly labelled as "monitoring", at least not in terms of what the EU Commission refers to as "monitoring in a legal sense"[23]. For instance, ENISA lacks the competence to analyse individual complaints. ENISA's objective was intended to be "observatory monitoring", formalised in the Regulation as "assistance and expertise" relating to network and information security within its competencies for the relevant institutions, bodies, and agencies of the Union (Article 2)[24]. The primary task of the Agency is, therefore, to collect, record, analyse, and disseminate relevant, objective, reliable and comparable information and data (Article 3).

ENISA's focus on providing advice and expertise characterises it as a governance body, relying on relationships within its expert networks and the efficient production of reliable data and information through statistics —typical features of governance. Although not explicitly outlined in its establishing text, ENISA aligns with the EU Commission's vision for the "better application of rules' through regulatory agencies, as outlined in the White Paper on European Governance under the heading better policies, regulation, and delivery"[25]. However, describing ENISA using governance language conceals the power relations of governmentality, obscuring its function as a monitoring body. The monitoring role becomes obscured in the governance language of "assistance" and "expertise".

Yet Louis Brun has interpreted the current post-regulation role of ENISA as guidance linked to its original monitoring mission[26]. Barrinha and Carrapico share a similar perception of ENISA's advisory function, suggesting that advice requires a normative assessment of the respective situation and is, therefore, a form of monitoring[27].

However, these critical analyses fall short. In this article, we delve into the power relations within ENISA's operational processes to illustrate how ENISA

human rights monitoring mechanisms: essays in honour of Jakob Th. Möller, Brill, Amsterdam, Boston, 2009.

[22] Para. 57 of the Preamble to the ENISA's Regulation of 2019 reads as follow: "The Management Board, composed of the representatives of the Member States and of the Commission, should establish the general direction of ENISA's operations and ensure that it carries out its tasks in accordance with this Regulation. The Management Board should be entrusted with the powers necessary to establish the budget, verify the execution of the budget, adopt appropriate financial rules, establish transparent working procedures for decision making by ENISA, adopt ENISA's single programming document, adopt its own rules of procedure, appoint the Executive Director and decide on the extension and termination of the Executive Director's term of office".

[23] For further references on this issue, see Schutterle, P., "Implementing of the EC State Aid Control-an Accession Criterion"*, Eur. St. Aid LQ*, Vol. 1, No. 1, 2002, p. 79 ff.

[24] Article 3, para. 1 of the ENISA's Regulation of 2019 reads as follow: "ENISA shall carry out the tasks assigned to it under this Regulation for the purpose of achieving a high common level of cybersecurity across the Union, including by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. ENISA shall act as a reference point for advice and expertise on cybersecurity for Union institutions, bodies, offices and agencies as well as for other relevant Union stakeholders".

[25] See also Egeberg, M., Trondal, J. and Vestlund, N.M., "The quest for order: unravelling the relationship between the European Commission and European Union agencies", *Journal of European Public Policy,* Vol. 36, No. 3, 2015, p. 609 ff.

[26] See Brun, L., *The role of the European Union Agency for Network and Information Security (ENISA) in the governance strategies of European cybersecurity,* available at: https://dial.uclouvain.be/memoire/ucl/en/object/thesis%3A16234.

[27] See Carrapico, H. and Barrinha, A., "The EU as a Coherent (Cyber)Security Actor?", *JCMS: Journal of Common Market Studies,* Vol. 55, No. 6, 2017, pp. 1254-1272.

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

is governing through discipline —it is exercising a form of monitoring that reveals relations of disciplinary power and governmentality.

III. ENISA'S CONTRIBUTION TO CYBERSECURITY OVERSIGHT

ENISA is involved in what Regulation 526/2013, now repealed by Regulation (EU) 2019/881 ("EU Cybersecurity Act")[28], regarding the European Union Agency for Network and Information Security (ENISA), described as providing "guidance, advice, and assistance" to the European Union institutions, bodies, offices, and agencies, as well as Member States, in developing policies on network and information security. We argue that these procedures essentially constitute a form of "monitoring", which, in our perspective, can be construed as "surveillance". Surveillance is implemented through governing and disciplinary processes involving identifiable tactics, techniques and operations inherent in ENISA's structure, operational methods and outcomes.

Structurally, the Agency operates through expert nodes at the EU and national levels. At the EU level, the five structural bodies of the Agency are the Management Board, Executive Board, Executive Director, Permanent Stakeholders' Group and a network of National Liaison Officers (NLOs)[29]. ENISA encompasses networks at the national level, and its group of legal experts reports on legal aspects of network and information security issues in all Member States, respectively[30].

The Agency's operational methods involve the collection of information and data, which it disseminates through its "products"[31]. ENISA's primary products include annual reports, thematic reports and surveys[32]. One significant thematic report is the study titled "Good Practices for Supply Chain Cybersecurity"[33]. Additionally, the Agency has recently produced a report titled "Artificial Intelligence and Cybersecurity Research", which, to our knowledge, is the first report of its kind at the EU level[34]. We use these reports to demonstrate how ENISA has developed its supervisory role.

ENISA employs good practice indicators to identify exemplary Member States in its 2022 report on good practices for information and communications technology (ICT)[35], as well as in the eleventh edition of the ENISA Threat Landscape (ETL) report[36]. In both reports, especially in the latter, ENISA develops sections on good practices, highlighting individual countries in bold, supported by data that validates their "good practice". For instance, in the domain of application-layer attacks, ENISA mentions the US and China as consistently ranking in the top positions, serving as both targets (US first, China second) and sources (US third, China first) of application-layer attacks[37]. Regarding HTTP DDoS attacks, ENISA specifically recognises the USA, China, Germany, Brazil and Russia as the main sources of HTTP DDoS attack traffic[38].

This focus on good practice indicators is essentially a kind of collaborative guiding and learning, or monitoring. Experts monitor member states and enforce strict adherence to a standard of good practice. In the cybersecurity discourse that ENISA has created, a "good Member State" is preferred over a "bad Member State". The consolidated annual activity report of 2021 introduces a new style and a different context, and the normalisation of good practice standards becomes even more pronounced[39]. The report introduces new key performance indicators and accompanying metrics. While the report indicates that these performance indicators and metrics serve the same function as good practice, it also highlights the effective achievements reached by Member States in the reported year. The selected practices are emphasised because they are activities that ENISA has implicitly identified as initiatives to be emulated; thus, ENISA's cybersecurity discourse is normalising

[28] Regulation (EU) 2019/881 OJ L 151, 7.6.2019, pp. 15-69.

[29] Chapter III, Art. 13 of the ENISA's regulation 2019/881.

[30] Chapter III, Article 23 of the ENISA's regulation of 2019.

[31] Chapter I, Article 4 of the ENISA' regulation of 2019.

[32] Chapter II, Article 5 of the ENISA's regulation of 2019.

[33] The text is available at the following address: https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity.

[34] The text is available at the following address: https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research.

[35] The text of the report is available at the following address: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

[36] *Ibidem*.

[37] *Ibidem*.

[38] *Ibidem*.

[39] The report is available at the following address: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

promising practices. Moreover, the 2021 annual report identifies developments in individual Member States in clear lettering throughout, making it easier to recognise those states that carry out good or promising practices that should be emulated.

Examples of Member States that have earned the "bad" practice label include, firstly, Portugal. A number of cyber events in 2022 raised questions about Portugal's participation in subpar cybersecurity measures as a Member State[40]. Stressing that "cybersecurity is a top priority", ENISA underscored this by reminding Portugal of various EU rules designed to safeguard security in this domain[41]. These regulations encompass the Directive on a common level of network and information security[42], the Cybersecurity Act[43] and the European Electronic Communications Code[44].

On 20 March 2023, ENISA issued a press release titled "ENISA Foresight Cybersecurity Threats for 2030"[45]. Through this release, ENISA aims to identify and collect information on future cybersecurity threats that could affect the Union's infrastructure and services, impacting its ability to keep European society and citizens digitally secure, as observed in the Portuguese case[46].

The Agency encourages national governments to enhance the integration of cybersecurity education into school curricula, emphasising the significance of cybersecurity in both the history and future of the EU. Essentially, ENISA is reinforcing the undesirable category of delinquency and the society of

[40] For further information on these incidents, please visit the official webpage of ENISA at the following address: https://www.enisa.europa.eu/.

[41] *Ibidem*.

[42] The NIS Directive stands as the inaugural EU legislation addressing cybersecurity, with its primary objective being to establish a consistent and elevated standard of cybersecurity across all Member States.

[43] See the EU Cybersecurity Act available at the following address: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

[44] The text of the Code is available at the following address: https://www.eud.eu/policy/eu-accessibility-legislation/european-electronic-communications-code/#:~:text=The%20EECC%20sets%20an%20EU,emergency%20number%20'112'.

[45] The text of this study is available at the following address: https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

[46] *Ibidem*.

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

delinquency. This stance is explicitly stated by ENISA in its aforementioned press report, where the Agency emphasises its goal to integrate best practices for identifying cybersecurity threats and challenges into national cybersecurity plans[47]. Moreover, with a similar objective, ENISA has recently established a working arrangement with the US Cybersecurity and Infrastructure Security Agency (CISA), concentrating on capacity-building, exchanging best practices and improving situational awareness[48].

Not only are the Member States under scrutiny, but also Union citizens and other entities collaborating with ENISA, such as NGOs. Citizens undergo examination through socio-legal methods like surveys and interviews, aiming to gather information about the extent to which they exemplify the ideal citizen —one who has not encountered any cyber-attacks[49]. ENISA has effectively documented the encounters with cyber-attacks experienced by citizens and businesses residing in EU Member States through these surveys. Using these findings, ENISA successfully assembled its initial cyber threat landscape for the health sector, with a specific emphasis on ransomware and data breaches. The report reveals a troubling reality regarding the challenges faced by the EU health sector during the reporting period, including widespread incidents of ransomware and data breaches.

Concerning NGOs, their behaviour is closely monitored. Furthermore, ENISA collaborates with NGOs and other civil society institutions to enhance their expertise and awareness of cybersecurity[50]. ENISA extends invitations to NGOs and private sector stakeholders involved in cybersecurity at national, European and international levels to partake in the designation process of National Cybersecurity Certification Authorities (NCSS) and governance models[51]. The criteria consist of, for instance, a pledge from NGOs and stakeholders to enhance cybersecurity in Europe and a proven role deemed

[47] *Ibidem*.

[48] Further information is available at the ENISA's official website.

[49] See ENISA's Raising Awareness of Cybersecurity, also available at the following address: https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity

[50] See Agency for National Cybersecurity, 'ENISA Executive Director at ACN headquarters', available at: https://www.acn.gov.it/portale/en/w/il-direttore-esecutivo-di-enisa-nella-sede-di-acn

[51] Further information is available at the following address: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

"critical to the vital functions of society". These criteria act as evaluative measures, conditioning NGOs to consistently qualify as suitable participants in ENISA's processes.

As a result, disciplinary power operates on cybersecurity subjects in dual ways: firstly, it delineates an undesirable classification of a "bad Member State", and concurrently, it shapes the sought-after secure and safe identity of Europe, encompassing the cyber-secure Member State and the suitable NGO participant. The establishment of the unsuitable or socially non-vital category is intriguing due to its political utility. Crafting an identity for a Member State labelled as cyber-unsecure and an NGO lacking social representation provides a benchmark against which broader society can define itself, streamlining the oversight of the entire cybersecurity domain. Essentially, it allows for the oversight and control of the EU's cybersecurity sector by presenting a vision of a European Union where every member of society can enjoy cybersecurity, in contrast to being labelled as cyber-unsecure.

Therefore, the use of surveillance as a means of disciplinary power turns it into a normalising force. The following standards are derived from ENISA's surveillance schema. First, the European Union, and by extension ENISA, as a cyber-safe haven standard. Second, the society of cyber security is shaped in opposition to the "other", the society of cyber risk or insecurity. Thirdly, ENISA shapes the normalised subjects of a safe and secure society: the good member state and the reputable civil society institution.

This acknowledgment is significant because it casts doubt on the notion that ENISA is only a tool for advancement or a lighthouse for cybersecurity. An analysis of the Agency's operations demonstrates that it functions as a governing body, enforcing regulations. For instance, it uses information gathered and shared by intricate, self-organising networks of expert players to generate expert reports on innovative best practices under the National Cyber Security Strategies (NCSS)[52]. Here, it is important to remember that this structure depends on the normalisation of two unwanted categories: the Member State that is not safe online and the non-essential NGO in society. Collectively, these classifications lead to the development of an extremely undesirable cyber-unsecure society, which serves as the benchmark for the European cyber-secure and safe society.

[52] See the official ENISA website at the following web address: https://www.enisa.europa.eu/

Peace & Security – Paix et Sécurité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

IV. THE PREVENTION OF UNWANTED RISKS OF THE GENERATION OF GUARANTEE BACKSLIDINGS AND UNDUE STRATIFICATIONS

As critical examinations of the history of international law have posited, throughout its history there have been hegemonic attempts to use it as a tool both to segregate in terms of who its subjects are and who is excluded, and to assign greater or lesser entitlements and burdens to those who have been classified across different strata. This, for instance, was the case with the nineteenth-century classification of groups as either civilized, uncivilized, or "barbaric"[53].

Furthermore, it has been considered that the later and contemporary absence of a similar form of formally stratifying the addressees in different "castes", which would be more consistent with both the identification of Statehood in a post-Montevideo Convention era with the principle of sovereign equality —to the extent that all States with the basic requirements for being considered as such enjoy that guarantee—, is regretfully sometimes not sufficiently honoured in practice.

In this sense, it has been considered that the practical reference to "failed" versus other States, or to "rogue" or "evil" and other States, among other distinctions, in spite of being more political than an expression of international law, can make some more likely to being exposed to the imposition of certain harsh measures and unequal treatments, even though those imposing those sanctions —of questionable legality sometimes, when they do not meet the conditions of countermeasures or lawful sanctions under human rights law[54]— do not always do so consistently but rather heed alliances and sympathies, or strategical convenience with double standards. All of this recalls problematic historical events that had allegedly remained in the past[55].

And certainly, as evidence of the double standards and hypocrisy goes, a critical analysis can shed light on how those who are not deemed to be

[53] Remiro Brotóns, A. et al., *Derecho internacional: curso general*, Tiran Lo Blanch, Valencia, 2010, pp. 48-49, 458, 466, 689, 802.

[54] Cf. Articles 49 through 53 of the International Law Commission's articles on the Responsibility of States for Internationally Wrongful Acts, adopted in 2001; Committee on Economic, Social and Cultural Rights, General Comment No. 8, *The relationship between economic sanctions and respect for economic, social and cultural rights*, 1997, paras. 10-16.

[55] Remiro Brotóns, A. et al., *op. cit.*, pp. 59, 720, 798-802.

Peace & Security – Paix et Sécurité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

"rogue" sometimes engage in conduct that is seriously contrary to peremptory law, such as the prohibition of aggression. This would show that the tool of making lists, can be employed in ways that serve domination patterns or that are based on an implicit derision of certain bodies. So far, we have not focused on the intentionality behind making such lists: they can be well-meaning in terms of attempting to accomplish some objectives seen as adequate. But if these lists or classifications are not properly carried out, for instance in terms of verifying or ensuring due process guarantees, as the Kadi case before the European Court of Justice reminds about[56] and as we will discuss in this section, they can be both illegitimate and wrongful, depending on which kind of normativity they fail to observe.

It is important to bear in mind the aforementioned considerations, because the possible identification of a given actor as not being worthy of endorsement, and the potential labelling of some States as having a "bad practice" or the consideration of NGOs as being "unsuitable", are not without repercussions, both symbolic and practical. The composition and "governance" practice of ENISA is one based on expertise, and the agency is supervised by its Management Board concerning the implementation of its periodic programming, and the European Ombudsman when it comes to its operations[57]. We argue in this section that apart from this supervision, complementary means of oversight are required.

The potential serious implications of decisions made by the agency are an issue of concern. For instance, failure to obtain an EU Cybersecurity Certification schemes can be problematic for those wanting to effectively participate in European markets, notwithstanding the voluntary nature of participation in them[58]. Adverse consequences should not be thought of exclusively as encompassing "formal sanctions" and adverse judgments. That would be a narrow conception that fails to consider all the implications of interaction with institutional languages such as the legal one and the effects its use can generate.

[56] Remiro Brotóns, A. et al., *op. cit.*, p. 404.

[57] See Articles 3, 15, and 46 of the Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA.

[58] Further information is available at the following address: https://certification.enisa.europa.eu, accessed 26 January 2024.

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

We do not mean to suggest that certifications are inappropriate. Certainly, the identification of possible risks in terms of cybersecurity when it comes to software can be necessary in order to address an undeniable issue of concern. However, global administrative law analyses shed light on the reasons why rule of law guarantees must be applicable to standardization and certification schemes[59], and accordingly ought to be protected, both at the level of their design and implementation.

In this sense, for instance, it should be possible to challenge or contest the adequacy of the motivation of the frameworks on the basis of which the evaluation is carried out, *i.e.*, in light of which conduct will be evaluated. Doing so permits to ascertain if those frameworks are themselves defective and ought to be modified in order to be more consistent with technical or other considerations, and should thus encourage authorities at the European Union level to permit requests to reconsider and redesign cybersecurity standards taken into account by ENISA when this is in order, and to allow challenges as to their adequacy —especially in the evolving cyberspace field. Furthermore, the challenging, by those affected, of an evaluation carried out by ENISA over a given product —*e.g.*, software— or entity, in terms of whether there was an appropriate or rather faulty assessment, ought to be permitted in direct terms, *i.e.*, allowing those potentially affected to ask ENISA to reconsider, or being informed before the publication of an implicit or explicit evaluation of performance and adequacy with cyber security standards in order to allow contestation and permit eventual reconsiderations. In sum, both the standards handled by ENISA and its specific evaluations should be subject to possible reconsideration remedies or requests.

On the other hand, it must be conceded that it is true that governmental participation in an institution that carries out certification or identification of good practices would not eliminate the risk of strategical refusals or evaluations towards partnerships with non-governmental and the observance of standards, as has been demonstrated by the existence of allegations that NGOs have not been given consultative status at the ECOSOC due to

[59] Kingsbury, B., "The Concept of 'Law' in Global Administrative Law", *European Journal of International Law*, Vol. 20, No. 1, 2009, pp. 36-41; Kingsbury, B., Krisch, N. and Stewart, R.B., "The Emergence of Global Administrative Law", *Law and Contemporary Problems*, Vol. 68, No. 3/4, 2005, pp. 24-25.

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

ideological or political opposition by some State delegations[60]. The problems are hence not exclusive to technocratic bodies as ENISA —composed of management and executive boards, an executive director, an advisory group, and national liaison office networks[61]. However, as those criticisms against the respective practice show, it would be important to count with specific remedies permitting the challenging of decisions contrary to the granting of a given status to a potential or actual participant.

There have been some claims presented against ENISA at the European Union level, for instance related to public procuring, access to reports, and to contractual issues (labor, contracts, mobility, etc.), among others —some of which have already been the object of recommendations or decisions, with the rest pending them[62]. But while the waiting for a decision to be reached takes place, the implications of a given assignation of a status, including that of not having practices or being unsuitable, is problematic if there is no specific remedy addressing it or permitting the review of the decision.

In this regard, two clarifications are in order. Firstly, that even if an entity is not portrayed as having bad practices, the potential implications of not being among those with good practices can implicitly be problematic and generate prejudicial effects in terms of relationships and participation in European cyberspace dynamics, given exclusion or reluctance by others. This requires that due process guarantees be observed, as rule of law criteria recalled by global administrative law remind —as mentioned above. Secondly, it must be mentioned that even if failures to identify an entity as one having good practices take place "merely" in reports that are not binding decisions in themselves but have the nature of guidance, guarantees towards them are still in order. This is because such publications can still produce impacts affecting those mentioned in them, for example due to the expressive effects[63] that such publications can have. This is because their generation is not necessarily limited to adjudicative processes but to all instances of interaction with normative standards —the relevance of which should not be underestimated[64].

This does not eliminate the supervisory capacities of ENISA and makes its actions subject to scrutiny in order to prevent abuses or to permit correcting mistakes. This would actually strengthen its legitimacy, rather than weakening it. Mere "effectiveness" of power is not something that makes an entity legitimate and fair.

As Andrea Bianchi seems to suggest, the determination of what is epistemologically appropriate can also be the outcome of power relations[65]. This could be the case, in our opinion, on what is publicly "known" about the adequacy of a given State or organization, or even of certain *practices*, in terms of cyber security conduct —again, even not being mentioned amongst those with good practices is a form of frowning upon an entity, with public effects,

[60] Cf. UN Watch, *U.N. Denies Status to Christian Charity after China Objects*, 27 July 2009, available at: https://unwatch.org/un-denies-status-to-christian-charity-after-china-objects/; International Service for Human Rights, *Committee on NGOs must stop blocking NGO participation at UN through unfair tactics*, 14 June 2023, available at: https://ishr.ch/latest-updates/committee-on-ngos-continues-to-block-ngo-access-to-un-through-unfair-tactics/; International Service for Human Rights, *ECOSOC votes to grant 7 long-deferred NGOs consultative status*, 28 July 2023, available at: https://ishr.ch/latest-updates/ecosoc-votes-to-grant-7-long-deferred-ngos-consultative-status/; United Nations, *Continuing its Session, Non-Governmental Organizations Committee Recommends Status to 2 Entities, Rejects 5, Postpones Consideration of 93 Others*, 22 May 2023, available at: https://press.un.org/en/2023/ngo961.doc.htm, all accessed 26 January 2024.

[61] Article 13 of Regulation (EU) 2019/881 of the European Parliament and of the Council, of 17 April 2019.

[62] European Data Protection Supervisor, Decision in compliant case 2019-1135 against the European Union Agency for Cybersecurity (ENISA), 11 January 2021; European Ombudsman, Decision on how the European Union Agency for Cybersecurity (ENISA) carried out two staff selection procedures in the field of cybersecurity (cases 1159/2021/VB and 1224/2021/VB), 16 December 2022; European Ombudsman, The lack of reply to a request for a copy of the recording of a second hearing in an administrative inquiry carried out by ENISA, Case opened on 17 January 2024; European Ombudsman, How the European Union Agency for Cybersecurity (ENISA) carried out two staff selection procedures, 16 December 2022; European Ombudsman, Recommendation of the European Ombudsman in case 723/2018/AMF on how the European Union Agency for Network and Information Security handled a public tender procedure, 4 October 2019; European Ombudsman, Decision of the European Ombudsman closing his inquiry into complaint 131/2009/ELB against the European Network and Information Security Agency, 23 November 2010; General Court of the European Union, Ninth Chamber, Case T-322/21, Order, 23 December 2023.

[63] Sunstein, C. R., "Law's Expressive Function", *Law and the Good Society*, Vol. 144, No. 3, 1999, pp. 55-58.

[64] Lasswell, H.D. and MC Dougal, M.S., "Trends in Theories About Law: Comprehensiveness in Conceptions of Constitutive Processes", *The George Washington Law Review*, Vol. 41, No. 1, pp. 1972-1973, 2-13.

[65] Bianchi, A., *International Law Theories*, Oxford University Press, Oxford, 2016, p. 21 ("The primary function of epistemic communities is to fix the terms of the discourse and shape the way in which we look and think […] ").

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

which are not generated only in adjudicative procedures. Furthermore, these considerations shed light on how not only entities, but also the mentioning of certain practices as adequate or not ought to be contestable, given possible mistakes or debates as to the latter as well.

Therefore, given the need to provide guarantees against abuses of power or errors by means of due process standards as contestation, and publicness requirements such as the need to motivate observations by ENISA —which, in turn, facilitate challenging them[66]—, we consider that it would be convenient for the practice in that regard to have the following two assurances: a) on the one hand, rather than permitting wide labellings as adequate or not, to simply indicate in reports the perceived deficiencies in practice by stressing that this evaluation is advisory and based on the perceptions by ENISA, subject to contestation and change based on evolving practice and state of the art considerations. Secondly, b) in terms that are similar to the periodic review mechanisms at the United Nations, ENISA should strive to adopt and publicize evaluations *only* after it has heard a given subject and permitted it to contest preliminary observations that are critical of its cyber security positions, in the case of entities; or after it has debated and heard different positions in the case of evaluating a debatable standard on whether a given practice is seen as adequate or not.

Furthermore, the risk of backsliding(s) must be kept in mind. Elaborating on our consideration that the constant perception of being watched can be problematic, one can argue that the desire to not be seen as "at fault" and worthy of being branded as an actor with bad practices can generate stimuli making a subject long to be seen as behaving appropriately —in terms of compliance[67]. This, coupled with social conduct-inducive dynamics as acculturation and socialization[68], can make a State or NGO adopt practices seen as innovative or even *avant-garde* in terms of strong cyber security programmes and policies. These practices, however, can be problematic when seen from the lenses of privacy, freedom of expression, and other human rights considerations. Eventual problematic practices, when endorsed by ENISA and seen as worthy

[66] Kingsbury, B., *op. cit.*, pp. 32-33, 41-50.

[67] Koh, H.H., "Internalization through Socialization", *Duke Law Journal*, Vol. 54, No. 3, 2005, pp. 976, 978-979, 981.

[68] *Ibidem*.

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

of or requiring emulation by all European Union members, could thus lead to a race to the bottom in which they are consolidated and promoted.

However, such a results-oriented perspective with security as the paragon standard on the basis of which the conduct is measured can lead to ignoring important safeguards, such as those found under human rights law mentioned above, among others. It is pertinent to mention that in the past it has been said by human rights supervisory bodies and agents that certain States have breached their obligations in the field during their counter-terrorism measures —in the application of which human rights duties must be observed[69]. It must be added that human rights guarantees are applicable and in the cyberspace and require respect and protection in it[70]; and that there are some specific manifestations of how they are to be respected and protected in that domain, as has been identified by United Nations and Inter-American supervisory bodies; with the Inter-American Commission on Human Rights even saying that cybersecurity measures can help to promote human rights —when used properly, we might add[71].

[69] Inter-American Commission on Human Rights, *Report on Terrorism and Human Rights*, 22 October 2022, paras. 54, 56; Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní, A., "Impact of counter-terrorism measures on civil society and civic space, and counter-terrorism-based detention", 10 October 2023, para. 8; Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní, A., "Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism", 1 March 2023, paras. 2, 20, 31; UNITED NATIONS, *Basic Human Rights Reference Guide: Conformity of National Counter-Terrorism Legislation with International Human Rights Law*, 2014.

[70] Seatzu, F. and Carrillo Santarelli, N., "Towards a Strengthening of Non-Interference, Sovereignty, and Human Rights from Foreign Cyber Meddling in Democratic Electoral Processes", *Brooklyn Journal of International Law*, Vol. 49, No. 3, 2023, p. 609.

[71] Committee on the Rights of the Child, General Comment No. 25, *Children's rights in relation to the digital environment*, 2 March 2021, paras. 4, 14, 25-26, 60, 77, 81-82, 92, 104, 112, 116-117 ("The rights of every child must be respected, protected and fulfilled in the digital environment"); Human Rights Committee, General Comment No. 34, *Freedoms of opinion and expression*, 12 September 2011, paras. 12, 15, 39, 43-44 (on "electronic and internet-based modes of expression" as being protected); Inter-American Commission on Human Rights, *Standards for a Free, Open and Inclusive Internet*, 15 March 2017; Inter-American Commission on Human Rights, *Freedom of Expression and the Internet*, 31 December 2013, para. 117 ("public policies to promote *cybersecurity* and ensure the privacy of information are important measures for reaching […] objectives" of human rights law).

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

The looming risk of wrong assessments can perversely end up encouraging actions in which European actors strive to "toughen up" their practices and put security ideas at the forefront, perhaps without paying due consideration to human rights and other criteria. These dynamics can become entrenched in terms of their emphasis to pre-empt negative assessments that are always present in the minds of the respective agents. In turn, when they internalize these considerations, the standards they internally promulgate can be the product of a perceived constant surveillance in which a certain form of paranoia leads to the desire to show performance and "results" from the security angle if other applicable standards are not likewise sufficiently emphasized. Conversely, emphasizing in the reports by ENISA that human rights are also relevant would help to prevent human rights backsliding temptations. As an example of a commendable example of an ENISA comment in line with these considerations, one can cite how it said that:

> The spyware industry has boomed further and this type of borderline-illegal software remains a threat to all of us. In ways to legitimise their products this industry often claims that their services are intended to focus on criminals and terrorists, whereas in fact they regularly target journalists, politicians and political opposition as well as human rights activists. And while surveillance technologies can serve a purpose, there are rising concerns about privacy, human rights, transparency, accountability and ethical considerations. There is a trend from public and private entities to take action and address these concerns[72].

If reminders as the previous one about the importance of striving to ensure cyber security in ways that are compatible with fundamental rights and guarantees were absent, ironically, States and NGOs could be swayed to support cyber security dynamics in which privacy or measures against persecution or the collection of cyber evidence of crimes, among others, are not given sufficient safeguards. These practices could encourage replication and internalization in internal security measures, thereby generating an organizational-like atmosphere at those levels as well. All of this could happen in the name of tackling the complexities of security challenges in the cyber space if sufficient guarantees are not duly considered, as a result of rushed or exclusively security-concerned policies and publications.

Therefore, addressing the sources of cyber security threats must always pay due attention to the necessity of doing so in a way that is compatible with fundamental due process and substantive safeguards and guarantees that exist for the sake of human rights and other fundamental interests. And ENISA can set the example in this regard.

Doing so would discourage narrow perspectives that ignore the risks of security discourses that do not pay sufficient attention to the implications of fundamental rights in the course of actions allegedly carried out for the sake of their defence.

Otherwise, internal cyber security policies and measures could generate an internal constant state of alert as well, which can have detrimental freedom of expression and other effects. Considering how misunderstandings can exist, for example in terms of differing opinions and the fear that having the politically wrong ones in a given polity can be seen as disruptive or inappropriate in spite of them being debated, there is no small cause of concern of comments made in the cyberspace being misinterpreted and leading to persecution. The accommodation of challenges and debates in the elaboration and evaluation of ENISA reports, as suggested above, can help to shed light on those potential problems if they discuss human rights guarantees, as we suggest in the current text.

In this regard, one must remember that human rights case law insists that bothersome opinions are still protected by freedom of expression. And that freedom, along with privacy and other rights, must be respected by cyber security actions. There is a risk that an emphasis only on security results can make some lose this of sight to its full extent if it loses of sight that security should be oriented towards the protection of those rights, and in ways that are respectful of them. Moreover, a rights-sensitive mindset can not only help to avoid the risks identified in this section, but also lead to increasing awareness of the relevance of human rights in the cyberspace in ways that lead to the design of actions that end up enhancing their protection, for instance against cyber-bullying.

V. CONCLUSION

One major actor in the modern governance change seen throughout the EU is ENISA. At the outset, the monitoring role of ENISA —which was characterised as an observatory role— was seen as guidance and support rather than legal monitoring at the institutional or academic levels. We reveal that

[72] ENISA, *ENISA Threat Landscape 2023*, October 2023, at 34. Emphasis in the original.

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

ENISA's current position operates as a monitoring body, where monitoring is synonymous with surveillance. The disciplinary character of ENISA's cybersecurity discourse is highlighted when one interprets the Agency's job as surveillance.

ENISA functions as a supervisory site, with cybersecurity serving as the focal point of the code of discipline. Cybersecurity discourse generates standardised identities and exerts influence over the identities of EU citizens, Member States and other groups like national and international NGOs. The notion of the EU as a safe and cybersecure society and ENISA's identity as a cybersecurity advocate are normalised, as is the organisation's acknowledgement as a security body.

In addition to being a cybersecurity institution that provides support and information to the EU and its member states, ENISA has also become a powerful tool for states. A closer look shows that ENISA has not stopped monitoring; On the contrary, it now carries out surveillance activities using punitive measures.

Interpreting ENISA as an example of a supervisory cybersecurity model is important for two reasons.

Firstly, because this implies that the proliferation of cybersecurity debates in the European Union, leading to discussions regarding governance in the ENISA model, should not be automatically regarded as "progress" for the international community. Instead, as argued in this article, we should examine the means by which this "progress" has been facilitated. In the context of ENISA and the EU, it has transpired through the employment of governance discourse to address cybersecurity issues. This has led, contrary to the EU's assertions, not to reduced government but improved governance: a form of governance that is automatic, permanent, and unseen, executed by networks of experts who do not take on responsibility but generate information and data, presented in the form of statistics that come to define the EU's cybersecurity situation.

Secondly, this article describes the nature of ENISA's cybersecurity as a discipline of practice: cybersecurity is both a moral standard, the goals we need and a conversation of governance and discipline.

We would like to emphasise once again that the criticism we express here is not about ENISA, which supporters of cybersecurity will see as an independent organisation dedicated to improving the performance of cybersecurity across Europe. Instead, it aims to critique practices of cybersecurity by creating claims of progress and independence from the state. This is not a negative review; ENISA is an efficient, advanced, and useful supervisory mechanism that allows for the expansion of the EU cybersecurity model.

However, we believe that ENISA cannot be called a "beacon of cyber protection". By constantly reviewing ENISA's processes, we try to focus on the operation of the policy in institutions and how it affects personal rights, in order to support dissent and opposition to this model.

Therefore, we need to ask how the best ENISA cybersecurity strategy is designed. What signs are successful in the process and what is the thinking behind this development being considered "progress"? Who should be responsible or who should be the expert responsible for the discipline? This is the only way we can critique other aspects of cybersecurity: disciplinary and regulatory capacity, and where this capacity can be used to enforce our rights against ENISA, the EU, member states and their inhabitants.

Finally, we consider that the motivations behind the constitution of ENISA, when coupled with human rights sensitivities, can contribute to the design of practices in the reporting and other operations that it carries out so as to strengthen the protection of fundamental guarantees. Otherwise, failing to properly bearing the relevance in mind could encourage practices that are problematic from a due process perspective and also from the point of view of consistency with foundations that European Union law should always keep in mind, including those mentioned in the Charter of Fundamental Rights of the European Union[73].

BIBLIOGRAPHIC REFERENCES

ALFREDSSON, G., GRIMHEDEN, J., RAMCHARAN, B. and ZAYAS, A. (eds.), *International human rights monitoring mechanisms: essays in honour of Jakob Th. Möller*, Brill, Amsterdam, Boston, 2009.

ARMSTRONG, K.A., "Rediscovering civil society: the European Union and the White Paper on Governance", *European Law Journal*, Vol. 8, No. 1, 2012, pp. 102-132.

[73] See articles 1, 7, 8, and 11 of the Charter of Fundamental Rights of the European Union, among others.

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204

BACKMAN, S., "Risk vs. threat-based cybersecurity: the case of the EU", *European Security*, Vol. 32, No. 1, 2023, p. 85 ff.

BENDIEK, A., BOSSONG, R. and SCHULTZE, M., *The EU's revised cybersecurity strategy: half-hearted progress on far-reaching challenges*, Deutsches Institut für Internationale Politik und Sicherheit, Berlin, 2017.

BRANDÃO, A. and CAMISÃO, P., "Playing the Market Card: The Commission's Strategy to Shape EU Cybersecurity Policy", *JCMS: Journal of Common Market*, Vol. 60, No. 5, 2022, pp. 1335-1355.

BRUN, L., "The role of the European Union Agency for Network and Information Security (ENISA) in the governance strategies of European cybersecurity", Master's thesis, Université catholique de Louvain and Université Saint-Louis, 2018.

CHAMON, M., *EU Agencies: Legal and Political Limits to the Transformation of the EU Administration*, Oxford, 2016.

CHAMON, M., "EU Agencies: Does the Meroni Doctrine Make Sense?", *Maastrich Journal of European and Comparative Law*, Vol. 17, No. 3, 2010, p. 281 ff.

GÖRISCH, C., "Die Agenturen der Europäischen Union", *JURA-Juristische Ausbildung*, Vol. 38, No. 4, 2012, p. 10 ff.

HOUT, W. (ed.), *EU Strategies on Governance Reform: Between Development and State-building*, Sweet and Maxwell, London, 2012.

KINGSBURY, B., KRISCH, N. and STEWART, R.B., "The Emergence of Global Administrative Law", *Law and Contemporary Problems*, Vol. 68, No. 3/4, 2005, pp. 24-25.

KOPCHEV, V., "The European Union Moves Ahead on Cybersecurity Research Through Enhanced Cooperation and Coordination", *Information & Security: An International Journal,* Vol. 43, No. 3, 2019, pp. 67-81.

MITRAKAS, A., "The emerging EU framework on cybersecurity certification", *Datenschutz und Datensicherheit – DuD*, Vol. 42, No. 2, 2018, p. 411 ff.

SEGURA, A., *El desafío de la ciberseguridad global*, Tirant lo Blanch, Valencia, 2023.

TOVO, C., *Le agenzie decentrate dell'Unione europea*, Naples, 2016.

VOS, E., "Reforming the European Commission: What role to play for EU agencies?", *Common Market Law Review*, Vol. 37, No. 5, 2000, pp. 1113-1134.

Peace & Security – Paix et Securité Internationales
ISSN 2341-0868, No 12, January-December 2024, 1204
DOI: http://dx.doi.org/10.25267/Paix_secur_int.2024.i12.1204