Cyber Security Frameworks (CSFs): An Assessment Between the NIST CSF v2.0 and EU Standards

Manisha Parmar
NATO Cyber Security Centre
NCI Agency
The Hague, Netherlands
manisha.parmar@ncia.nato.int

Dr. Andy Miles
Made to Measure Mentoring
Surrey, United Kingdom
andymiles@m2m2.co.uk

***Abstract*— The rapid increase in volume and sophistication of Advanced Persistent Threats (APTs) bring growing threat of attack on critical Communications and Information Systems (CISs). This risk prompts practitioners in the field of Cyber Security to baseline CIS to achieve a targeted security posture and perform continuous assessments to ensure both maintenance and improvements to this posture. This is especially vital in the defence industry given the criticality of CIS to mission assurance in the Air, Land, Sea and Space domains. Security in Space, which has been recognized as NATO's newest operational domain, is vital to ensure commensurate practices are upheld to support the Space Commander with their missions. To do this, a Cyber Security Framework (CSF) can be leveraged. CSFs "…provide guidelines and best practices for developing, implementing, and maintaining a cybersecurity program tailored to an organization's needs." [1] Standardization of a single framework for use does not, however, exist. This paper compares the commonly adopted and broadly used NIST CSF v2.0 [2] with a standard emerging from the European Union to compare suitability and identify gaps to ensure holistic cyber security coverage for the defence sector where Cyber is viewed as an enabler to missions in the Space domain.**

Keywords— Cyber Security Framework, CSF, NIST, standardization, NIS2 Directive, NATO, ESA

I. Introduction

NATO provides support to various missions in the kinetic domains of Air, Land, Sea and, as NATO's newest domain, Space. Cyberspace capabilities, and by extension, the security of these capabilities, underpin the Commander's objectives and provides mission assurance. To achieve a requisite security posture, security practitioners aim to baseline key Communications and Information Systems (CISs) by using one or more Cyber Security Frameworks (CSFs). CSFs "…provide guidelines and best practices for developing, implementing, and maintaining a cybersecurity program tailored to an organization's needs." [1]. A single, internationally recognized CSF does not, however, exist. Many refer to widely adopted national standards such as the CSF produced by the National Institutes of Standards and Technology (NIST), the NIST CSF version 2.0 [2] is currently in review and soon to be released. With a standard emerging from the US, the European Union (EU) has also aimed to create and standardize similar products, starting with the Network and Information Systems Directive 2 (NIS2 Directive) [4], which is aimed at EU Nations / organizations to achieve a minimum standard of cyber security maturity. Given these two emergent standards, it is worthwhile for organizations such as NATO and the European Space Agency (ESA), with Member States / partnerships from both North America and Europe, to understand these products for suitability and identify their gaps in order to adopt and align holistic security practices for their CISs. This paper compares and contrasts the NIST CSF v2.0 with the NIS2 in order to inform and aid security practitioners in their use to achieve a minimum baseline noting that a baseline is "the minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity and/or availability protection." [3]

This paper is structured into Sections. After this Introduction [Section I], Section II offers an overview of the NIST CSF v2.0 while Section III gives an overview of the NIS2 Directive. Section IV then identifies and describes the alignment and deltas across both products with Section V providing an overall summary of findings. Section VI describes the authors' recommendations given findings based on Sections IV and V. Section VII summarises the conclusions.

II. NIST CSF v2.0

The NIST CSF version 2.0, which is planned for public, official release in early 2024, succeeds the NIST CSF version 1.1 [5] which was released in 2018. It is not within scope of this paper to compare the deltas between version 1.1 and 2.0 but the reader is encouraged to review the ample gap assessments available such as those offered by [6] and [7]. The NATO Communications and Information Agency (NCIA) developed a CIS Security Capability Breakdown [8] based on the earliest version of the NIST CSF (version 1.0, released in 2014) [9]. This Breakdown has acted as the NATO customized CSF but given it is over 10 years old, a new, updated CSF is required.

NIST created the CSF v2.0 to aid organizations with the following three outcomes: 1) to Understand / Assess, 2) to Prioritize and 3) to Communicate. The tool is intended to help organizations develop profiles to assess current state, target state and community agreed profiles which underpin an organization's ability to realize these outcomes.

The Framework, while developed by a United States (US) government funded entity (NIST), indicates that it is appropriate for use by organizations also outside of the US. While the generic taxonomy presented is easily adoptable in an international setting, the Framework demonstrates strong

alignment with US strategic initiatives such as the Executive Order on Securing Critical Infrastructure [10] and the US National Strategy on cyber security [11].

The Framework is presented using functions (shown and described in Table I) with described outcomes coupled to implementation examples indicating that the functions must be achieved concurrently and in a continuous fashion. While functions and outcomes (desired effects) can be considered relatively static, the implementation examples are rapidly changing. It is for this reason that the implementation examples are maintained separately, online.

TABLE I. NIST CSF V2.0 FUNCTIONS AND DESCRIPTIONS [2]

Function	Description
Govern	"Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy. The GOVERN Function is cross-cutting and provides outcomes to inform how an organization will achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations."
Identify	"Help determine the current cybersecurity risk to the organization. Understanding its assets (e.g., data, hardware, software, systems, facilities, services, people) and the related cybersecurity risks enables an organization to focus and prioritize its efforts in a manner consistent with its risk management strategy and the mission needs identified under GOVERN."
Protect	"Use safeguards to prevent or reduce cybersecurity risk. Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events."
Detect	"Find and analyze possible cybersecurity attacks and compromises. DETECT enables timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse cybersecurity events that may indicate that cybersecurity attacks and incidents are occurring."
Respond	"Take action regarding a detected cybersecurity incident. RESPOND supports the ability to contain the impact of cybersecurity incidents."
Recover	"Restore assets and operations that were impacted by a cybersecurity incident. RECOVER supports timely restoration of normal operations to reduce the impact of cybersecurity incidents and enable appropriate communication during recovery efforts."

Take, for example, the case of identity management within the Protect function. Identity management, when an organization can authenticate individuals, can be implemented using Role Based Access Control (RBAC) [12], Attribute Based Access Control (ABAC) [13], Zero Trust Architecture (ZTA) [14] or several other means. The Framework provides standardization to describe 'what' but does not prescribe any single method to describe 'how'.

NIST suggests the use of tiers to rate or assess the requisite or desired maturity for a CIS. Appendix B of [2] describes the tiers across the Governance, Management and Third Party Supplier perspectives however a generic description of the four tiers is provided in Table II.

TABLE II. NIST CSF V2.0 TIERS AND DESCRIPTIONS [2]

Tier	Description
Tier 1	**Partial**; risk management practices are generally unstructured and ad hoc. Risks are unassessed and the organization functions with stakeholders (internal and external) on a case by case basis thereby lacking consistency.
Tier 2	**Risk Informed**; risk management practices are documented and organizations are informed, however, there is lack of repeatability and still lack of consistency.
Tier 3	**Repeatable**; risk management practices are consistently applied and reoccurring consistent. The organization has thereby achieved a holistic approach to security practices.
Tier 4	**Adaptive**; risk management practices are consistently applied and continuously assessed in order to ensure not only maintenance but regular improvement to adopted approaches and application. There is strong consistency and discipline to security practices.

Profiles and their corresponding tier (both achieved or targets) will be different based on the criticality of the CIS and subsequent residual risk level. CISs providing key mission services may need to reach Tier 4 where CISs providing services without mission impact (employee timesheet system, for example) may only require Tier 2 achievement. It is, therefore, necessary for an organization to review and assess risk using another methodology (not included in the Framework). While the Framework identifies the Identify function as one way for an organization to assess risk, organizations can supplement this process by adopting "crown jewel" and risk assessment methodologies such as the widely adopted ones provided by Mitre Corporation[1] [15], [16].

The outcomes of these activities result in products which can be abstracted or further detailed, depending on the audience in which communication with stakeholders should occur. Governance communities and "C Suite" executives do not typically require details beyond understanding operational impact where technical stakeholders will desire deeper detail to inform their tasks and duties. It is the responsibility of the assessor to create reporting products fit for purpose to the various communities. The Framework provides template recommendations but does not inform this part of the process in significant background.

[1] The methodologies provided by Mitre are only examples; several other entities provide approaches based on similar principles and desired outcomes.

There are, of course, limitations of the Framework which must be considered before adoption [17]. For starters, it has attracted criticism that the Framework assessment is subjective and may not render the same results with different assessors. Furthermore, the Framework is voluntary and does not result in any type of certification by a management authority (unlike the ISO 27001 standard [18]). Lastly, the Framework provides a mechanism for organizations to baseline but it may not be enough for an organization and its mission, recalling that a baseline is only a minimum standard and there is no single standard that can cover all of the specific needs of every organization. Additional CSFs / standards will apply, especially in niche areas. Some CISs may warrant added protection that goes beyond the provisions of NIST and it is necessary for an organization to know their own environment, mission and threats in order to adequately manage risk. For example, in the NATO context, additional CSFs focused on the defence industry could be leveraged, such as the Information Technology (IT) Security Guidance, IT Security Risk Management: A Lifecycle Approach prepared by the Communications Security Establishment from the Canadian Department of Defence [19]. ESA may want to consider space standards emerging from bodies such as the European Cooperation for Space Standardization (ECSS) and their Space Engineering: Security in Space Systems Lifecycles [20]. The additional coverage, if any, provided by either of these standards is outside of scope for this assessment but would be required to determine suitability commensurate with the desired CIS robustness to achieve (the target ambition).

III. NIS2

The Network and Information Security (NIS) directive v2.0 is a European Union (EU) Directive which stipulates minimum controls for critical CIS in EU Nations. The Directive is not a framework itself, however, Nations are expected to develop their own CSFs using the Directive as a foundation. While several Nations have developed their own frameworks and reference the importance of the NIS2 (such as the French Critical Infrastructure Information Protection Framework [21]), it is unclear whether the NIS2 Directive has specifically been integrated at the national level. Future work to understand use and adoption of the Directive within EU countries may include analysis against National CSFs but is outside the scope of this paper.

NIS2 is an update to the original 2016 version which has attracted criticism for leading to fragmentation between Member Nations, and fragmentation between these Nations can lead to vulnerabilities within EU cooperation. Thus, this new Directive has been drafted to reduce disparity between members and to benchmark maturity. While a comparison between the NIS2 and its previous version is outside of scope for this paper, it would be interesting to note the significant differences to determine whether fragmentation concerns and challenges have indeed been resolved.

Enhanced focus on information sharing and cooperation protocols are likely the areas where maturity has been increased. This seems implied in Paragraphs 8 and 9 of the Directive which cite lack of applicability of the Directive on organizations operating in national and/or public security, defence, etc., noting specifically those involved in the prevention, detection and prosecution of criminal offences are exempt. Subsequently, there are limitations on the aspects of information sharing and collaboration within this auspice indicating third party disclosure is not required and National sovereignty continue to be a priority upheld by the Directive.

A report conducted by Deloitte in 2022 [22] identities four key topics related to the NIS2: 1) Risk Ownership, 2) Security Requirements, 3) Supply Chain Security and 4) Incident Reporting. These topics are certainly one valid approach to grouping the directives within the NIS2 and are elaborated as follows:

Risk Ownership:

- National strategy for cyber security and single points of contact for communication including aspects of governance within Member States.

Security Requirements:

- Cyber security risk management activities which focus on cyber hygiene, access control, use of cryptography for network security, Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP).
- Information sharing arrangements (both across and within Member States) on cyber-attacks and breaches in a timely fashion to reduce the overall exposure of Member States.
- Maintenance of domain registrations and registry of entities such as Domain Name Server (DNS) entities.

Incident Reporting:

- Establishment of national Computer Security Incident Response Teams (CSIRTs) to perform monitoring, dynamic risk assessments and ensuring situational awareness. In addition, CSIRTs are also to perform incident handling and management, and carry out reporting within and across Member States,
- Reporting standardization (both across and within Member States) on vulnerabilities and remediation activities and for CSIRT engagement with the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe) [23],

Supply Chain Security:

- Supply chain considerations for organizations operating within the EU.

The NIS2 appears to lean towards certification preferences citing the ISO standard in several places for general practices and cloud security protections vs the corresponding NIST publications. Thus, making it even more obvious that the Directive is not intended for consideration only, but is targeting compliancy by Member States. It may, however, fall short of achieving this goal given Nations are recommended to implement CSFs based on the Directive and there is no audit procedure or formalized certification attached to the Directive. Member States are provided guidelines for self-audit and ensuring compliancy within their own nations. In essence, the Directive is mandatory but not strictly enforced by a body outside of any Member State. Lastly, the Directive is ultimately intended for cyber practitioners to implement but is written from a legal standpoint (language wise) leaving room for interpretation and ambiguity. Considering Nations are to draft their own CSF based on the Directive, the desire to reduce fragmentation is counter acted by the various flavours of CSF which have or will emerge.

IV. Comparison Between NIST CSF v2.0 and NIS2

With an independent understanding of both the NIST CSF v2.0 and the EU's NIS2 Directive, the products can be compared.

Beginning first with the similarities, both products aim to provide a minimum baseline or standard when it comes to cyber security capabilities and ensuring robustness in how these capabilities are implemented by entities. Both have been drafted in recent timelines (NIST CSF v2.0 is expecting release in early 2024 and the NIS2 directive was released in December 2022). Both recognize the importance of Governance which aligns with the People, Process and Technology paradigm of organizational success as described in [24]. The People, Process and Technology dimensions are underpinning to success in organizations given the dependency and the need to take considerations across all three perspectives.

Most interesting, however, is that neither is "implementable" using the standalone product and both prescribe either a follow-on Action Plan (in the case of NIST CSF v2.0) or subsequent CSF(s) (in the case of NIS2) and one can assume a further Action Plan would be required. Thus, both products exist as part of the same process (achievement of a Cyber Security Programme) but appear to be targeted for different purposes.

A high-level assessment conducted in [25] reviewed the NIST CSF v1.1 security functions and aligned the various parts of NIS2. Given the NIST CSF v2.0 security functions are different, this assessment may no longer be accurate but is used in consideration of this assessment. Table III identifies the parallels between NIST CSF v2.0 and the NIS2.

TABLE III. NIST CSF v2.0 and NIS2 Alignment

NIST CSF v2.0 Function	Alignment with NIS2
Govern	Creation of national strategies for cyber security and establishing mandated ways of working within EU nations and across EU Member States. Establishment of a single point of contact within each nation and ensuring reporting is done across CSIRTs and the EU-CyCLONe. Establishing mandated third-party reporting and information disclosure upon incidents. Ensuring information sharing agreements are put in place. NIST CSF v2.0 includes supply chain considerations under governance although there is a separate NIST publication for supply chain risk management [27].
Identify	Asset management to be undertaken by Member States and identification of vulnerabilities to be undertaken as a part of a member state's security requirements. The NIS2 requirements about information sharing (for threat intelligence, vulnerabilities, and mitigations) would also align to this category.
Protect	Aligned direction to the NIS2 set of security requirements related to network security (protection of Data In Transit [DIT], identity management and NIS2 specific requirements on multi factor authentication, as well as requirements for user training and awareness programs.
Detect	Corresponds to the NIS2 requirement to have CSIRT teams perform network monitoring activities and detect incidents. CSIRT teams are also required to maintain situational awareness, and this is heavily related to the ability to Detect (anomalies in the CIS).
Respond	CSIRT teams are required to both respond and report on incidents as they occur, including the ability to reduce negative effects on CIS under attack. The NIS2 identifies the need for a BCP and this aligns with the Respond function (within the Incident Management category).
Recover	NIS2 indicates the need for the DRP which aligns with the execution of the incident recovery plan prescribed in NIST.

There is a strong relationship between the content of the NIST CSF v2.0 and the NIS2, however, there are also noteworthy differences. Beginning with some of the most obvious, NIST's Framework is drafted by a US body which is funded by the US Government and while it is preferred for US based adoption, it is applicable for international use and adoption as well. NIS2 is developed by the EU and is applicable to EU Member States. Further, adoption of the NIST Framework is intended as a set of best practices or recommendations (not mandatory) where, the NIS2 is intended as a mandate with delegated enforcement. EU Member States are expected to comply with the Directive by October 2024 and the Directive should be codified at the national level within the EU Nations.

The focus of the NIS2 Directive is on collaboration and cooperation between Member States and, thus, has a very strong information sharing and collaboration nature. The requirements for third party disclosure and mandated reporting are certainly not included in the NIST Framework given the differences in target audience and adoption.

The NIST CSFs (all versions) are intended to provide best practices and set a common taxonomy for cyber security where the NIS2 Directive is intended as a regulatory document (intended for codification at the national level) that Nations must legally comply with. Both require the eventual

development of an Action Plan to realize outcomes and the NIS2 recommends further derivation of the embedded directives into one or more CSFs. The EU does not propose use of an existing CSF nor has it indicated any plans to create and provide CSF(s) aligned to the Directive.

Given the regulatory nature of the NIS2, NIS2 also puts specific Key Performance Indicators (KPIs) in place for reporting related to incident management. Organizations have twenty-four hours to provide an early warning report and must follow up in seventy-two hours with the official incident response. One month later, a final incident report must be issued or the CSIRT can release an interim report if the investigation is ongoing. The NIST CSF v2.0 does not include any KPIs and suggests that development of the Action Plan be used by the organization to capture both KPIs and Key Risk Indicators (KRIs) to monitor, evaluate and inform a strategy. Strategy is also mentioned and is an element assumed as a prerequisite by the NIST CSF v2.0 but prescribed for creation by the NIS2.

To take this one step further, NIS2 identifies potential penalties to be laid on organizations should compliancy with the Directive not be put in place. This audit and, if necessary, corresponding penalty remain the responsibility of the member state. While it may be desirable for the EU to take a stronger, leading role in the area of enforcement, from a pragmatic perspective, it must rely on strong cooperation with Member States given the number of Nations and included organizations. EU laws and legislations are upheld by the European Commission as described in [26], Enforcing EU Law for a Europe that Delivers, which indicates that the European Commission has expanded authority to uphold EU laws and that "a key way in which it discharges this role is by working with Member States, as well as monitoring their implementation and application of EU law." [26].

V. Summary

While, from a content perspective, there is alignment between the NIST CSF v2.0 and the NIS2 Directive, the nature of the products (how and when they are used) is quite different. Further, both products require additional artefact development to properly leverage and implement (ultimately, the Action Plan).

The NIST CSF v2.0 is a best practice / taxonomy support document while the NIS2 Directive is intended to be codified and enforced at the national level within EU Nations.

The NIST CSF will require an Action Plan to be realized and is most likely preceded by one or more directives and a Strategy. The NIS2 must be succeeded by Strategy and the production of one or more CSFs until, finally, an Action Plan can be developed.

The overall flow for product development is shown in Figure 1, where NIS2 is considered a Directive and the NIST CSFs are considered as a type of CSF. A CSF should ultimately be derived from one or more directives and perhaps the EU should consider the development of an EU CSF, to complement the NIS2.

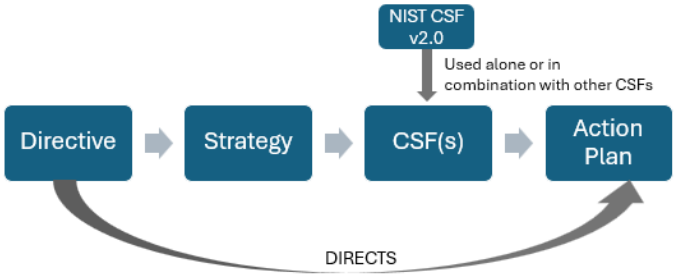

Fig. 1. Artefacts for Implementing Cyber Security Programme

The NIST CSFs are developed in the US but are intended for international adoption should any Nation or organizational entity choose to use it.

The NIS2 is a Directive developed by the EU and is enforced for compliancy by EU Nations via the European Commission. The adoption of NIS2 is not optional for EU Nations. While there is nothing constraining a non-EU from using content from the NIS2, there is no legal or compliancy aspect of enforcement to non-EU Nations.

VI. Recommendations

All products shown in Figure 1 (Directive, Strategy, CSF(s) and Action Plan) could be developed by any entity - a Nation belonging to NATO, ESA, both or neither), an organization within a Nation, NATO or ESA themselves (as international organizations), etc.

At the organizational level, given there could be multiple memberships to different bodies, some with governance functions (like the EU) or other relationships (like with NATO, ESA or both), there may be multiple directives to comply with and several adoptions of various CSFs. Given the number of products and the potential lack of understanding between their content and application, organizations will ask themselves – will their organization reach NIS2 compliancy if using the NIST CSF v2.0 (or even v1.1)? Given the summary of differences as described in Section V, the answer will be "not necessarily", and this compliancy cannot be implied through use of a NIST recommended CSF with follow on Action Plan. This is because the NIST CSF v2.0 (or any version) could be preceded by other Directives (with potentially conflicting rules) and the subsequent Action Plan may not necessarily align. Additionally, at this point, the EU have not developed their own follow on CSF from the NIS2 and this leaves a certain degree of flexibility for Member States.

Nations facing this same question at the national level will need to assess for themselves whether their existing (should they have one) Action Plan meets the NIS2, regardless of whether it was derived from the NIST CSF v2.0 or some other CSF(s). Once this assessment is completed, augmentation to the Action

Plan can be identified and put in place for compliancy. If no Action Plan exists, one should be created.

Further, EU Nations which hold membership in NATO and/or ESA, will want to know how their NIS2 compliancy (which is mandatory) could aid alignment of the activities undertaken with NATO and/or ESA. It seems the NIST CSF v2.0 is a very good place to start given the content alignment and that Nations should further develop their Action Plan in compliancy with the NIS2 Directive. Essentially, the Nation can adopt both the NIS2 and the NIST CSF v2.0, with development of their own Strategy and Action Plan.

The EU may want to consider endorsing use of the NIST CSF v2.0 or developing another CSF which Nations can adopt, to aid with national compliancy to NIS2.

NATO and ESA should consider the NIST CSF v2.0 to achieve a minimum baseline for their systems and augment this baseline with specific recommendations emerging from their respective domains. NATO, given Space is an operational domain and ESA could consider the adoption of the ECSS Security in Space standard [20] alongside, should it be considered by Space SMEs as appropriate and suitable. Furthermore, supporting commercial / industry partners to organizations such as NATO or ESA should also consider their own alignment to both NIST and NIS2 in order to satisfy requirements on the customer side – it could possibly be a strategic advantage.

Both NATO and ESA will require the development of an Action Plan to realize the security functions from the Framework and uphold adopted organizational directives. If NATO and/or ESA Nations (regardless of whether they are EU Nations or not) could align their national action plans with the ones derived by NATO and ESA, this will reduce different, or worse, incompatible, KPIs and KRIs from being measured, reported, and updated. The challenge, however, will be in cases where NATO or ESA directives are contrary to the NIS2, however, given the regulatory nature of NIS2 and the fact that Nations are not regulated to comply with NATO or ESA directives, the NIS2 will take precedent for these EU Nations.

VII. Conclusions

The achievement of a minimum cyber security baseline can start with adoption of a CSF and the NIST CSF v2.0 Framework appears a reasonable place for organizations, Nations and international organizations such as NATO and ESA to consider.

Recalling the definition of a baseline, organizations seeking maturity beyond a baseline ambition may seek to augment their cyber security posture with other, more specific, guidance, such as the standards emerging from the space standardization lifecycle [20]. Organizations such as NATO or ESA may seek to bolster their CIS environment through use of domain specific guidelines to extend beyond just a minimal baseline, especially for mission critical CIS, however, use of the NIST CSF v2.0 for achieving the minimum baseline is effective.

There is significant content overlap between best practices recommended by NIST and the regulatory directives listed in the NIS2 from a content perspective.

The use of these products, however, fits in different places of an overall process to be undertaken by Nations or organizations in a Cyber Security Programme. While adoption of the NIST CSF v2.0 can certainly help limit the gap in gaining NIS2 compliancy (for those EU Nations regulated to do so), this is only one step of the process. Organizations and EU Nations will need to ensure action plans are created to realize the NIS2 Directive and, furthermore, if a Strategy is not already in place, it will be required. While the NIST CSF v2.0 is created in the US for US based organizations, its adoption can be internationally relevant. It is not, however, mandatory for NATO, ESA, or EU Nations.

If NATO and/or ESA Member States could align their national action plans with the ones derived by NATO and ESA, or vice versa, this will reduce different, or worse, incompatible, KPIs and KRIs from being measured, reported, and improved. It will also bring additional coherency and reduced fragmentation across nations with membership in multiple organizations such as the EU, NATO and ESA.

References

[1] N. Poggi, “Cybersecurity Frameworks 101 – The Complete Guide”, Prey Project, January 23, 2024. https://preyproject.com/blog/cybersecurity-frameworks-101. Accessed December 28, 2023.

[2] National Institutes of Standards and Technology, “Public Draft The NIST Cybersecurity Framework 2.0”, National Institute of Standards and Technology, August 8, 2023. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf. Accessed on February 4, 2024.

[3] NIST Computer Security Resource Center Glossy, “Glossary”, National Institute of Standards and Technology, https://csrc.nist.gov/glossary. Accessed on February 20, 2024.

[4] Official Journal of the European Union, “Network and Information Systems Directive 2”, European Union, 14 December 2022, in press

[5] National Institutes of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity v1.1”, National Institute of Standards and Technology, April 16, 2018 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Accessed on February 7, 2024.

[6] NIST Cyber Security Framework, “Updating the NIST Cybersecurity Framework – Journey to CSF 2.0”, National Institute of Standards and Technology, https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20. Accessed on February 7, 2024.

[7] Securicon Team, “What’s new in NIST’s Cybersecurity Framework (CSF) 2.0|, Securicon, August 16, 2023. https://www.securicon.com/whats-new-in-nists-cybersecurity-framework-csf-2-0/. Accessed on February 7, 2024.

[8] G. Hallingstad, L. Dandurand, “Cyber Defence Capability Framework – Revision 2”, NATO Communications and Information Agency (NCIA), September 2010.

[9] National Institutes of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity v1.0”, National Institute of Standards and Technology, February 12, 2014. https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf. Accessed on February 7, 2024.

[10] US Gov Info, “Executive Order 13636, Improving Critical Infrastructure Cybersecurity”, United States Government, February 12, 2013.

[11] The White House, “Cybersecurity Strategy”, United States Government, 13 March 2023.

[12] R. Sandhu, “Role-based Access Control”, Elsevier Science Direct, Volume 46, Pages 237 – 286. 1998.

[13] V. Hu, R. Kuhn, D. Ferraiolo, J. Voas, "Attribute-Based Access Control," in *Computer*, vol. 48, no. 2, pp. 85-88, Feb. 2015, doi: 10.1109/MC.2015.33

[14] NIST Special Publication 800-207, “Zero Trust Architecture”, National Institute of Standards and Technology, August 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf. Accessed on February 25, 2024.

[15] Mitre Corporation, “Crown Jewels Analysis”, Mitre Corporation, January 4, 2024.

[16] Mitre Corporation, “ATT&CK”, Mitre Corporation, https://attack.mitre.org/. Accessed February 25, 2024.

[17] M. Teplinksy, “A Review of NIST’s Draft Cybersecurity Framework 2.0”, September 13, 2023. https://www.lawfaremedia.org/article/a-review-of-nist-s-draft-cybersecurity-framework-2.0. Accessed February 24, 2024.

[18] International Standards Organization, “ISO/IEC 27001:2022”, International Standards Organization, October 2022.

[19] Government of Canada, “IT Security Risk Management: a Lifecycle Approach, Overview ITSG-33” Communications Security Establishment Canada, November 2012.

[20] European Cooperation for Space Standardizaion (ECSS), “Space Engineering: Security in Space Systems Lifecycle”, ECSS, May 25, 2023.

[21] The French Cybersecurity Agency (ANSSI), “The French CIIP Framework”, November 30, 2023. https://cyber.gouv.fr/en/french-ciip-framework. Accessed February 12, 2024.

[22] Deloitte, “The NIS2 Directive, How Organizations can Prepare”, Deloitte, https://www2.deloitte.com/nl/nl/pages/risk/articles/the-nis2-directive.html. Accessed on February 23, 2024.

[23] European Union Agency for Cybersecurity (ENISA), “CyCLONe, European Cyber Crises Liaison Organisation Network,” https://www.enisa.europa.eu/topics/incident-response/cyclone. Accessed on February 14, 2024.

[24] M. Prodan, A. Prodan, “Three New Dimensions to People, Process, Technology Improvement Model”, Research Gate, March 25, 2019, in press

[25] I. van Gemert, “Mapping NIST to the NIS2 EU Directive”, LinkedIn Blog Post, January 3, 2023, https://www.linkedin.com/pulse/mapping-nist-nis2-eu-directive-igor-van-gemert/. Accessed February 23, 2024.

[26] European Commission, “Enforcing EU Law for a Europe that Delivers”, European Commission. October 13, 2022.

[27] National Institutes of Standards and Technology, “Cybersescurity Supply Chain Risk Management Practices for Systems and Organizations”, National Institute of Standards and Technology, May 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf. Accessed on February 23, 2024.