

A cyber hygiene readiness model for network digital twins in telecommunication infrastructure

Levon Petrosian^{1,†}, Viktor Gnatyuk^{2,*,†} and Roman Jasek^{3,†}

¹Individual Entrepreneur Petrosian Levon H., Kyiv, 01135, Ukraine

²State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Maksym Zaliznyak Str., 3, Kyiv, 03142, Ukraine

³Tomas Bata University in Zlin, T. G. Masaryk Sq., 5555, Zlin, 76001, Czech Republic

Abstract

Network Digital Twins (NDTs) can support analysis, diagnosis, emulation, and control of modern telecommunication infrastructure. However, when an NDT becomes connected to real operational data and recommendations, it also becomes a cyber-sensitive component of the operator environment. Poor data hygiene, unclear ownership, weak access control, unprotected synchronization interfaces, or unvalidated recommendations can make the twin unreliable or unsafe even before advanced attacks are considered. This paper proposes CHR-NDT, a Cyber Hygiene Readiness model for NDTs in telecommunication infrastructure. The model defines eight readiness dimensions, four maturity levels, a compact readiness profile, and an optional risk-gap interpretation. The dimensions cover telemetry and data hygiene, synchronization and interfaces, identity and access control, model and data integrity, recommendation validation, logging and auditability, incident response and recovery, and governance. The model is aligned with NDT architecture concepts and with cybersecurity, maturity, and cyber-resilience guidance from ITU-T, 3GPP, ISO/IEC, NIST, ENISA, and ETSI. The paper also provides an author-created architecture scheme, a mapping to NIST CSF 2.0, and a 5G Core/MEC-oriented use case with attack scenarios. CHR-NDT is not a replacement for a full security audit, but it gives operators and researchers a simple structure for discussing whether a network twin is ready for operational use with acceptable cyber hygiene.

Keywords

Network Digital Twin, cyber hygiene, telecommunication infrastructure, cyber resilience, readiness model

1. Introduction

Telecommunication infrastructure is becoming more complex because operators have to manage physical network elements, virtualized functions, cloud and edge resources, software-defined control, and large volumes of operational data. A Network Digital Twin (NDT) is one possible answer to this complexity. In simple terms, an NDT is a digital representation of a real network that uses operational data, models, and interfaces to support analysis, diagnosis, simulation, and sometimes control of the physical network [1, 2].

This makes NDTs attractive for planning, troubleshooting, capacity management, and future zero-touch network operation [3]. At the same time, an NDT can create a new operational risk. Recent survey work on digital twin networks also treats privacy and security as important open issues for this network paradigm [4]. If the data in the twin is stale, incomplete, or manipulated, the twin may give wrong recommendations. If synchronization interfaces are weakly protected, attackers may influence the flow between the physical network and the virtual representation. If there is no clear human approval process, an NDT recommendation may be applied too quickly in a critical infrastructure context. Therefore, cyber hygiene should be checked before an NDT is treated as an operational support tool.

Cyber hygiene is used here in a practical sense: basic and repeatable security practices that reduce avoidable risk. This idea is close to ENISA's view of cyber hygiene as a way to improve everyday

WCH'26: Fifth International Workshop on Cyber Hygiene, June 25–26, 2026, Krakow, Poland

*Corresponding author.

† These authors contributed equally.

✉ kievlevon@gmail.com (L. Petrosian); gnatyukvo@gmail.com (V. Gnatyuk); jasek@utb.cz (R. Jasek)

🆔 0009-0006-0551-9137 (L. Petrosian); 0000-0002-4916-7149 (V. Gnatyuk); 0000-0002-9831-9372 (R. Jasek)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

cybersecurity practices across organizations [5]. For NDTs, cyber hygiene cannot be limited to passwords or antivirus-like measures. It must also cover telemetry quality, model updates, synchronization, auditability, and responsibility for decisions produced with help from the twin.

The research question of this paper is:

How can a telecommunication operator check whether an NDT is ready for operational use from a cyber hygiene perspective before it is connected to operational decision-making?

To answer this question, the paper proposes a Cyber Hygiene Readiness model for NDTs. The contribution is intentionally practical. It is a structured checklist with readiness levels and evidence examples, not a mathematical resilience index and not a taxonomy of attacks. This choice is important because many organizations need a first-step instrument before they can perform deeper testing, formal risk assessment, or advanced cyber-resilience engineering.

The paper makes three contributions:

- it formalizes NDT cyber hygiene readiness as a profile of eight dimensions and four levels;
- it maps the dimensions to NIST CSF 2.0 functions and adds a risk-oriented interpretation;
- it provides an author-created architecture scheme and an illustrative 5G Core/MEC use case with attack scenarios.

Unlike existing cybersecurity frameworks that address digital twins in a generic manner, the proposed CHR-NDT model introduces a telecom-oriented readiness structure specifically adapted to operational Network Digital Twins and their synchronization, recommendation, and governance workflows.

2. Background and scope

2.1. Network digital twin

ITU-T Recommendation Y.3090 defines a digital twin network as a virtual representation of a physical network that is useful for analysing, diagnosing, emulating, and controlling the physical network based on data, models, and interfaces [1]. The recommendation highlights several important elements for this paper: data collection, real-time mapping, models, standardized interfaces, security, privacy, and synchronization. ITU-T Y.3091 is also relevant because it treats capability levels and evaluation methods as a way to discuss the technical maturity of DTN systems [6]. ITU-T Y.3092 and 3GPP TR 28.915 further connect NDTs with management and orchestration in IMT-2020 and beyond networks, which is important for the telecom use case in this paper [7, 8].

Recent research also describes NDTs as data-driven models that can operate close to real time and support network management tasks [2]. In the 5G and beyond context, digital twins are discussed as tools for continuous assessment, monitoring, and proactive maintenance [9]. ETSI's ZSM work also connects network digital twins with more automated and zero-touch network management [3]. These directions show why the NDT is not only a research object. It may become part of the operational environment.

For this reason, the security and hygiene of an NDT must be treated as a practical deployment issue. A twin that only exists in a laboratory can be evaluated as a research prototype. A twin that consumes live operational data and gives recommendations to network engineers needs a different level of care.

2.2. Cyber hygiene and readiness

Cyber hygiene usually means basic security practices that are performed regularly and consistently. In organizations, such practices may include asset awareness, secure configuration, access control, patching, backup, logging, and incident response preparation. NIST CSF 2.0 provides high-level cybersecurity

outcomes for governance, protection, detection, response, and recovery [10]. NIST IR 8356 is useful for this paper because it discusses security and trust considerations that appear when digital twins are used for monitoring, simulation, testing, and control [11]. ITU-T X.2011 is especially relevant because it gives security guidelines for digital twin networks, including threats, requirements, and countermeasures for DTN layers and interfaces [12]. NIST SP 800-160 Volume 2 Revision 1 adds a cyber-resilience engineering view, where systems should be able to anticipate, withstand, recover from, and adapt to adverse conditions [13].

For telecommunication providers, ENISA's guidance under the European Electronic Communications Code and ENISA's NIS2 implementation guidance are also useful because they link security measures with implementation evidence and operational responsibility [14, 15]. ENISA's 5G threat landscape and 2025 threat landscape show why telecom security should be treated as a practical infrastructure issue rather than as an abstract IT topic [16, 17]. This is close to the idea of a readiness model: the question is not only whether a control is named in a policy, but whether it is actually implemented, monitored, and improved.

The proposed model is also positioned against two neighbouring maturity ideas. ISO/IEC 30186 provides a generic digital twin maturity model and guidance for maturity assessment, but it is not specific to cyber hygiene in telecom NDTs [18]. The SPEAR cyber hygiene maturity model shows that cyber hygiene maturity can be assessed in critical infrastructure, but its focus is smart grids rather than network digital twins [19]. CHR-NDT is therefore narrower: it adapts cyber hygiene readiness to NDT data, synchronization, recommendations, and governance. Recent digital twin security surveys support the same need to connect threats and requirements across DT layers [20].

2.3. Limitations of this paper

This paper does not propose a full threat taxonomy for NDTs and does not evaluate operational resilience with a complex numerical model. The optional risk-gap indicator introduced below is only an interpretation aid, not a replacement for formal risk assessment. The goal is narrower: to provide a simple readiness model that can be used before deeper technical testing or formal certification.

The model is designed for three situations:

- a research group prepares an NDT prototype for a telecom use case;
- an operator considers connecting an NDT to live operational data;
- a supervisor or reviewer needs a clear checklist to discuss cyber hygiene before deployment.

3. Design principles

The proposed model follows four design principles.

NDT-specific, but simple. The model must reflect the special structure of an NDT: physical network, digital representation, telemetry, models, interfaces, and recommendations. At the same time, it should be understandable to engineers and managers who are not specialists in every NDT component.

Evidence-based. A readiness answer should be supported by evidence. For example, it is not enough to say that access control exists. The assessor should be able to see role definitions, access logs, approval records, or test results.

Human decision responsibility. NDTs may support automation, but critical telecom decisions should have clear responsibility. The model therefore includes recommendation validation and governance as separate dimensions.

Useful before advanced security testing. Penetration testing, formal verification, and deep cyber-resilience engineering may still be needed. The model is a first-step readiness structure that helps detect basic gaps before those more expensive activities.

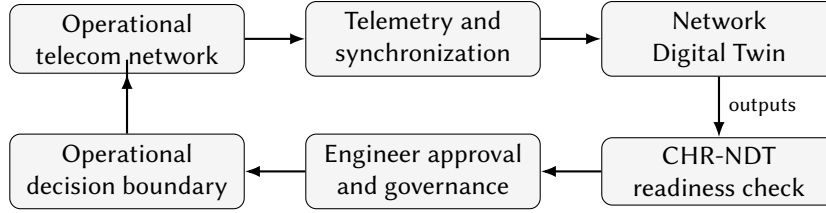


Figure 1: CHR-NDT position between the operational network, the Network Digital Twin, and the decision boundary.

4. Proposed cyber hygiene readiness model

The proposed Cyber Hygiene Readiness model for NDTs, abbreviated as CHR-NDT, consists of eight dimensions and four readiness levels. Each dimension can be checked separately. The result is not a single score. Instead, the model produces a readiness profile that shows which dimensions are ready and which require improvement.

Figure 1 shows the role of CHR-NDT. The model does not replace the NDT and does not directly control the physical network. It is placed between NDT outputs and operational decision-making so that cyber hygiene gaps are visible before recommendations are trusted.

4.1. Formal description

Let $D = \{D_1, \dots, D_8\}$ be the set of CHR-NDT dimensions. For each dimension D_i , the assessor checks available evidence E_i and assigns a readiness level $r_i \in \{0, 1, 2, 3\}$. The readiness profile is:

$$\mathbf{R} = (r_1, r_2, \dots, r_8).$$

CHR-NDT remains profile-based because a single number can hide weak dimensions. However, a simple risk-gap view can help interpretation. For each dimension, the gap is $g_i = 3 - r_i$. If a dimension has operational weight w_i , an optional normalized gap can be written as:

$$G = \frac{\sum_{i=1}^8 w_i g_i}{3 \sum_{i=1}^8 w_i}.$$

If no special weights are defined, all w_i are equal to 1. A high value of G means that many dimensions are still far from Level 3. This indicator is not a certification score; it is only a compact way to explain the readiness profile to engineers and managers.

4.2. Readiness levels

Table 1 presents the four readiness levels. The levels are intentionally simple. They help an assessor avoid a binary answer such as “secure” or “not secure”, which is usually too rough for real systems.

Table 1
Readiness Levels for CHR-NDT

Level	Name	Meaning
0	Ad hoc	The dimension is not defined, or it depends on individual habits without stable documentation.
1	Documented	Basic rules exist and responsible persons are named, but regular control is limited.
2	Controlled	Rules are implemented, monitored, and supported by evidence such as logs, tickets, test results, or access records.
3	Verified and improved	The dimension is regularly reviewed, tested, and improved after incidents, changes, or audits.

Table 2
CHR-NDT Dimensions and Examples of Evidence

ID	Dimension	What is checked	Example evidence
D1	Telemetry and data hygiene	Whether data sources are known, timely, complete enough, and protected from obvious quality problems.	Data source register; freshness checks; missing-data reports; data cleaning rules.
D2	Synchronization and interface hygiene	Whether physical-to-virtual and virtual-to-physical interfaces are documented, protected, and monitored.	Interface inventory; API authentication settings; synchronization logs; delay thresholds.
D3	Identity and access control	Whether users, services, and automated agents have defined roles and minimum necessary privileges.	Role matrix; account review; privileged access log; service account owner.
D4	Model and data integrity	Whether model versions, training data, configuration files, and topology data are protected from uncontrolled changes.	Version control; signed or approved model releases; change tickets; roll-back procedure.
D5	Recommendation validation	Whether NDT outputs are reviewed before they influence the physical network, especially for high-impact actions.	Human approval workflow; test sandbox; exception list; record of accepted and rejected recommendations.
D6	Logging and auditability	Whether important NDT actions can be reconstructed after an event.	Central logs; timestamps; operator IDs; audit trail for data import, model update, and recommendation use.
D7	Incident response and recovery	Whether the organization knows how to isolate, disable, restore, or rebuild the NDT after a cyber incident or data corruption.	Incident playbook; backup and restore test; isolation procedure; communication contacts.
D8	Governance and ownership	Whether business and technical responsibility for the NDT is clear.	Owner list; risk acceptance record; review schedule; policy link to telecom security management.

The main practical rule is conservative: an NDT should not be connected to operational decision-making if any critical dimension remains at Level 0. For higher-risk use cases, such as automated configuration changes or crisis response, most dimensions should reach Level 2 before use. The four levels are conceptually consistent with the NIST CSF 2.0 idea of progressively stronger risk-management posture, but CHR-NDT applies them per NDT-specific dimension rather than as an overall organizational tier.

4.3. Readiness Dimensions

Table 2 presents the eight CHR-NDT dimensions. They are derived from the structure of an NDT, from common cyber hygiene practices, and from cyber-resilience guidance.

The dimensions can be read as four operational blocks. D1–D2 check whether data and synchronization are reliable enough for a live or near-real-time twin. D3–D4 check whether access, model versions, topology data, and configuration data are controlled. D5–D6 check whether recommendations and logs can be reviewed before and after operational decisions. D7–D8 check whether the organization can recover from an NDT-related incident and whether responsibility for the twin is clear.

Table 3

Mapping of CHR-NDT Dimensions to NIST CSF 2.0 and Risk Meaning

ID	CHR-NDT focus	Main NIST CSF 2.0 relation	Risk-oriented interpretation if readiness is low
D1	Telemetry and data hygiene	Identify, Detect	The twin may use stale, incomplete, or manipulated data.
D2	Synchronization and interfaces	Protect, Detect	Attackers may influence the physical-to-virtual or virtual-to-physical flow.
D3	Identity and access control	Govern, Protect	Users, services, or tokens may receive excessive privileges.
D4	Model and data integrity	Identify, Protect	The operator may not know which model, topology, or data version is trusted.
D5	Recommendation validation	Govern, Protect	High-impact NDT outputs may affect the network without enough human review.
D6	Logging and auditability	Govern, Detect	Wrong recommendations or model changes may be impossible to reconstruct.
D7	Incident response and recovery	Respond, Recover	The organization may not know how to isolate or restore the NDT after compromise.
D8	Governance and ownership	Govern	Risk ownership, review frequency, and acceptance decisions may be unclear.

4.4. Mapping to NIST CSF 2.0 and risk meaning

CHR-NDT is not a replacement for NIST CSF 2.0, but it can be aligned with its governance, identification, protection, detection, response, and recovery logic. Table 3 presents a compact mapping and shows how low readiness can be interpreted as operational risk.

5. Illustrative telecom use case

Consider a telecom operator that wants to use an NDT for 5G Core and MEC-supported service management. The twin receives topology data, performance telemetry, configuration snapshots, slice-related status, and incident records from network management systems and from an SDN controller. It is expected to help engineers understand congestion, test possible changes, and recommend recovery actions for service slices or edge resources. The concrete operational boundary is an NDT-suggested slice reconfiguration or recovery action: it may be analysed offline, but it should not reach live SDN or orchestration workflows without approval.

Without a readiness check, the operator may focus only on model accuracy or visualization quality. These are important, but they do not answer basic cyber hygiene questions. For example, who can change the topology model? How fresh is the telemetry from the 5G Core and MEC environment? Can the NDT recommendation reach an SDN controller or orchestration tool? Are logs sufficient to explain a wrong recovery recommendation after an outage?

Table 4 shows how CHR-NDT can be applied before operational use.

In this example, the NDT should not yet be used for operational decision-making because D7 is at Level 0. This does not mean that the NDT prototype is useless. It means that the safe operational boundary should be limited. The operator may continue using the twin in offline analysis mode, while preparing an incident response and recovery procedure.

The same profile also gives a practical improvement plan. The first priority is to raise D7 from Level 0 to Level 1 or Level 2. The second priority is to improve D2, D4, and D6, because synchronization, model integrity, and auditability are directly connected to trust in the NDT. Governance should also be clarified before the system moves from a research or pilot mode to operational use.

Table 5 shows how the same use case can be connected to concrete attack scenarios.

Table 4
Example Readiness Profile for an NDT before Operational Use

ID	Dimension	Example level	Practical interpretation
D1	Telemetry and data hygiene	2	5G Core, MEC, and SDN data sources are registered; freshness is checked.
D2	Synchronization and interface hygiene	1	Interfaces are documented, but synchronization failure monitoring is incomplete.
D3	Identity and access control	2	User roles exist and privileged access is logged; service account review is scheduled.
D4	Model and data integrity	1	Model versions are named, but topology and slice-state changes are not fully approved through tickets.
D5	Recommendation validation	2	High-impact recommendations require engineer approval before any SDN or orchestration action.
D6	Logging and auditability	1	Logs exist, but they are not yet enough to reconstruct all model and recommendation updates.
D7	Incident response and recovery	0	There is no tested procedure for isolating or restoring the NDT after compromise.
D8	Governance and ownership	1	A technical owner exists, but risk ownership and review frequency are not formally approved.

Table 5
Example Attack Scenarios and CHR-NDT Response Logic

ID	Scenario	Main affected dimensions	Expected CHR-NDT response
A1	Poisoned telemetry reports false congestion in a slice or MEC segment.	D1, D2, D6	Check source freshness, missing-data reports, synchronization logs, and audit trail before trusting the recommendation.
A2	A compromised API token changes the synchronization flow between the NDT and an SDN-related system.	D2, D3, D6	Review interface authentication, service account owner, privilege scope, and logs of synchronization events.
A3	An unauthorized topology or model-version change makes the twin simulate the wrong network state.	D4, D6, D8	Verify model release records, topology change tickets, rollback procedure, and governance approval.
A4	The NDT recommends an aggressive recovery action that could affect live service continuity.	D5, D7, D8	Require human approval, test the recommendation in a sandbox, and confirm incident response and rollback readiness.

6. Discussion

The main advantage of CHR-NDT is that it is simple enough to be used early. It does not require a full attack simulation or a mature security operation center. It asks basic but important questions that are often skipped when a new technology is evaluated mainly by its functionality.

The model also helps separate three different questions:

- Is the NDT useful for network analysis?
- Is the NDT secure enough for its current use?
- Is the organization ready to take responsibility for decisions supported by the NDT?

These questions are related, but they are not the same. A twin can be technically useful and still not ready for live operational influence. A readiness model makes this distinction visible.

The model is also compatible with broader cybersecurity frameworks. NIST CSF 2.0 can be used to connect dimensions to governance, protection, detection, response, and recovery outcomes [10]. NIST

cyber-resilience guidance can support deeper engineering for systems that must withstand adverse cyber conditions [13]. ENISA telecom security guidance can support evidence-based assessment of measures in a provider environment [14]. The proposed model does not replace these sources. It adapts their logic to the specific structure of NDTs.

The model is also compatible with technical research where digital twins are used to detect abnormal or malicious behaviour in cyber-physical systems [21]. CHR-NDT does not compete with such detection frameworks. Instead, it asks whether the NDT environment itself has enough basic hygiene to make later detection, analysis, and response trustworthy.

There are limitations. First, the model is conceptual and illustrative. It should be tested on real NDT deployments or detailed case studies. Second, the readiness levels and risk-gap indicator are intentionally simple. This is useful for early assessment, but future work may define more precise evidence criteria for each level. Third, different telecom environments may require different priorities. For example, an NDT used only for offline planning has lower risk than an NDT connected to automated configuration workflows.

7. Conclusions

This paper proposed CHR-NDT, a Cyber Hygiene Readiness model for Network Digital Twins in telecommunication infrastructure. The model defines eight readiness dimensions, four maturity levels, a readiness profile, and an optional risk-gap interpretation. It focuses on practical cyber hygiene questions: data quality, synchronization, access control, model integrity, recommendation validation, logging, incident recovery, and governance.

The proposed model is useful as an early checklist before an NDT is connected to live operational data or decision-making. It does not replace a full security audit or detailed cyber-resilience engineering, but it helps identify basic weaknesses that can make a network twin unsafe. Future work should apply CHR-NDT to real or simulated telecom NDT deployments and refine evidence criteria for each readiness level.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

- [1] International Telecommunication Union, Recommendation ITU-T Y.3090: Digital twin network – Requirements and architecture, Technical Report, International Telecommunication Union, 2022. URL: <https://www.itu.int/rec/T-REC-Y.3090-202202-I/en>.
- [2] P. Almasan, M. Ferriol-Galmes, J. Paillisse, J. Suarez-Varela, D. Perino, D. Lopez, A. A. Pastor Perales, P. Harvey, L. Ciavaglia, L. Wong, V. Ram, S. Xiao, X. Shi, X. Cheng, A. Cabellos-Aparicio, P. Barlet-Ros, Network digital twin: Context, enabling technologies, and opportunities, *IEEE Communications Magazine* 60 (2022) 22–27. doi:10.1109/MCOM.001.2200012.
- [3] European Telecommunications Standards Institute, ETSI GS ZSM 018: Zero-touch network and Service Management (ZSM); Network Digital Twin for enhanced zero-touch network and service management, Technical Report, ETSI, 2024. URL: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/018/01.01.01_60/gs_zsm018v010101p.pdf.
- [4] A. Maradapu Vera Venkata Sai, C. Wang, Z. Cai, Y. Li, Navigating the digital twin network landscape: A survey on architecture, applications, privacy and security, *High-Confidence Computing* (2024). URL: <https://doi.org/10.1016/j.hcc.2024.100269>. doi:10.1016/j.hcc.2024.100269.
- [5] European Union Agency for Network and Information Security, Cyber Hygiene, Technical Report, ENISA, 2016. URL: <https://www.enisa.europa.eu/publications/cyber-hygiene>.

- [6] International Telecommunication Union, Recommendation ITU-T Y.3091: Digital twin network – Capability levels and evaluation methods, Technical Report, International Telecommunication Union, 2023. URL: <https://www.itu.int/rec/T-REC-Y.3091-202312-I/en>.
- [7] International Telecommunication Union, Recommendation ITU-T Y.3092: Digital twin for management and orchestration in IMT-2020 networks and beyond, Technical Report, International Telecommunication Union, 2024. URL: <https://www.itu.int/rec/T-REC-Y.3092-202409-I/en>.
- [8] 3rd Generation Partnership Project, 3GPP TR 28.915: Study on management aspect of Network Digital Twin, Technical Report Release 19, Version 19.0.0, 3GPP, 2025. URL: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4263>.
- [9] O. Holubnychyi, et al., Self-organization technique with a norm transformation based filtering for sustainable infocommunications within CNS/ATM systems, in: I. Ostroumov, M. Zaliskyi (Eds.), Proceedings of the 2nd International Workshop on Advances in Civil Aviation Systems Development, volume 992 of *Lecture Notes in Networks and Systems*, Springer Nature Switzerland, Cham, 2024, pp. 262–278. doi:10.1007/978-3-031-60196-5_20.
- [10] C. Pascoe, S. Quinn, K. Scarfone, The NIST Cybersecurity Framework (CSF) 2.0, Technical Report NIST CSWP 29, National Institute of Standards and Technology, 2024. URL: <https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20>. doi:10.6028/NIST.CSWP.29.
- [11] J. Voas, P. Mell, P. Laplante, V. Piroumian, Security and Trust Considerations for Digital Twin Technology, Technical Report NIST IR 8356, National Institute of Standards and Technology, 2025. URL: <https://doi.org/10.6028/NIST.IR.8356>. doi:10.6028/NIST.IR.8356.
- [12] International Telecommunication Union, Recommendation ITU-T X.2011: Security guidelines for digital twin network, Technical Report, International Telecommunication Union, 2024. URL: <https://www.itu.int/rec/T-REC-X.2011-202404-I/en>.
- [13] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, R. McQuaid, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, Technical Report NIST Special Publication 800-160, Volume 2, Revision 1, National Institute of Standards and Technology, 2021. URL: <https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final>. doi:10.6028/NIST.SP.800-160v2r1.
- [14] European Union Agency for Cybersecurity, Guideline on Security Measures under the EEECC, Technical Report, ENISA, 2021. URL: <https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc>.
- [15] European Union Agency for Cybersecurity, NIS2 Technical Implementation Guidance, Technical Report, ENISA, 2025. URL: <https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance>.
- [16] European Union Agency for Cybersecurity, ENISA Threat Landscape for 5G Networks, Technical Report, ENISA, 2020. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks>.
- [17] European Union Agency for Cybersecurity, ENISA Threat Landscape 2025, Technical Report, ENISA, 2025. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>.
- [18] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 30186:2025: Digital twin – Maturity model and guidance for a maturity assessment, Technical Report, ISO/IEC, 2025. URL: <https://www.iso.org/standard/53306.html>.
- [19] I. Skarga-Bandurova, I. Kotsiuba, E. Rios Velasco, Cyber hygiene maturity assessment framework for smart grid scenarios, *Frontiers in Computer Science* 3 (2021) 614337. URL: <https://doi.org/10.3389/fcomp.2021.614337>. doi:10.3389/fcomp.2021.614337.
- [20] H. Mun, K. Han, E. Damiani, H. K. Yeun, T.-Y. Kim, L. Martino, C. Y. Yeun, A comprehensive survey on digital twin: Focusing on security threats and requirements, *IEEE Access* 13 (2025) 73362–73390. URL: <https://doi.org/10.1109/ACCESS.2025.3563621>. doi:10.1109/ACCESS.2025.3563621.
- [21] E. C. Balta, M. Pease, J. Moyne, K. Barton, D. M. Tilbury, Digital twin-based cyber-attack detection framework for cyber-physical manufacturing systems, *IEEE Transactions on Automation Science and Engineering* (2023). URL: <https://www.nist.gov/publications/digital-twin-based-cyber-attack-detection-framework-cyber-physical-manufacturing>. doi:10.1109/TASE.2023.3243147.