

Mission-based Resilience

White Paper

Executive Summary

In this white paper, we discuss the mission-based resilience of cyber infrastructures, i.e., using the business mission decomposition and mapping of missions to assets to support decision-making and operate resilient services. In our case, a mission represents the business objectives of an organization and consists of abstract systems that should be operating in order to support such objectives. The systems are then mapped to particular cyber assets (hosts, services) for which we collect technical data, including the vulnerabilities they might have and cyber attacks they face. Modelling the missions gives us a precise idea of how exploitation of a vulnerability affects the organization and its business objectives. We showcase the implementation of our proposed approach in the Resilmesh system and discuss our experience in deploying in operational environments. Moreover, we comment on alternative solutions, compatibility issues, and harmonization efforts taken so far.

1. Introduction

Many organizations today rely heavily on complex, interconnected ICT infrastructures to carry out their operational objectives. As cyber threats increase in frequency and sophistication, traditional defenses focused purely on perimeter protection or component-level hardening are no longer sufficient. Instead, contemporary security paradigms have shifted toward **cyber resilience**, i.e., the ability to anticipate, withstand, recover from, and adapt to adverse conditions, attacks, or compromises on cyber resources. Crucial to this concept is a **mission-centric approach**, which evaluates and maintains cyber resilience not merely through technical metrics or isolated asset statuses, but in relation to the overarching operational missions and core business goals the underlying technology supports.

To operationalize mission-centric cyber resilience, structured modeling frameworks are necessary to map low-level cyber assets, dependencies, and vulnerabilities to high-level mission goals. Initial foundational concepts for mission-impact assessment were established in European research initiatives such as the **CRUSOE** project and further extended in the **Resilmesh** framework. These models construct dependency graphs and functional trees that quantify how cyber incidents degrade operational capabilities, allowing security operators to prioritize response and mitigation strategies based on mission criticality.

While custom dependency frameworks effectively serve specific cyber resilience architectures, widespread adoption and cross-domain interoperability depend heavily on standardization. Standardized formats for software and hardware composition, such as Software Bill of Materials (SBOM) and the CycloneDX standard, have gained significant traction for supply chain security and asset dependency management. However, key structural differences exist between general-purpose dependency representations and mission-centric models. In particular, the explicit logic dependencies used in mission modeling, such as the **AND/OR notation** applied within Resilmesh to represent redundancy and joint capability requirements, offer distinct expressive capabilities compared to the **required/optional** dependency relations standardized in CycloneDX. Comparing these formalisms is vital to bridging operational mission assurance with mainstream cybersecurity standards.

The remainder of this paper is structured as follows. Section 2 introduces the foundational mission model originally proposed in the CRUSOE project and refined within the Resilmesh initiative, detailing the conceptual mapping between cyber assets and mission objectives, and presents the architectural implementation of this mission-centric framework within the Resilmesh platform. Section 3 explores the standardization of mission models, providing a comparison between the Resilmesh model and CycloneDX. Section 4 concludes the paper.

Funded by
the European Union

2. Modeling missions

Modelling business missions and mapping them to cyber assets is a challenging task. Herein, we illustrate it on an approach taken in the Resilmesh project [Bernabe2025], specifically its ISIM and CSA components. This originates in the earlier CRUSOE project [Husak2022], but the Resilmesh approach receives a proper implementation as shown in the following section. Resilmesh's ISIM data model or earlier CRUSOE data model store information on the cyber assets, i.e., hosts and services in the network and their dependencies or vulnerabilities. However, mapping missions to cyber assets is a more complex issue that requires further tool support than what is already included in the CRUSOE data model or ISIM. CRUSOE/ISIM data model only models missions as entities and directly connects them to assets that support such missions. This allows for prompt listing of all assets supporting a mission or checking whether the asset is somehow relevant for any missions. However, there are more details to capture that are formulated and stored using a different approach, the CSA component.

2.1 Mission decomposition model

Mission decomposition stands on the following premises. A mission is decomposed into mission-supportive processes that are mapped to IT services that are consequently mapped to cyber components. Moreover, the mission is formally described as a system of *mission functional requirements* and *mission security requirements*. The functional requirements are posed on IT services by the mission-supportive processes and on cyber components by the IT services. The security requirements are expressed as desired levels of the CIA (e.g., *None, Low, or High*) posed on mission-supportive processes, IT services, and cyber components. A *satisfying mission configuration* is a subset of mission-supportive processes, IT services, and cyber components that align with the mission's functional requirements. Finally, *mission resilience* is the mission's ability to continue its operations while maintaining all the required functional and security requirements.

The mission decomposition model [Javornik2022] is a graph structure with the mission-supportive processes, IT services, and cyber components as nodes. The functional requirements are represented as edges between mission-supportive processes and IT services or between IT services and cyber components. The alternative mission configurations are expressed via the AND/OR nodes [Jakobson2014]. An AND node in a mission configuration poses a requirement for the presence of all of its child nodes. The child nodes represent either the supportive IT services or the cyber components. An OR node expresses a mission configuration option since it poses a requirement for the presence of at least one of its child nodes. For example, let us consider a mission-supportive process dependent on two IT services. In such a situation, an AND node is added to the model, the mission-supportive process is connected to the AND node, and the AND node is connected to the two IT services. The OR nodes or combinations of AND/OR nodes

are used similarly. A mission-supportive process may be satisfied by more mission configurations, i.e., combinations of IT services and cyber components. For example, a mission-supportive process dependent on one of the two IT services produces three satisfying mission configurations, one with the first IT service, one with the second IT service, and one with both. Finally, the edges between cyber components indicate network visibility of the components, i.e., a situation in which the two components can reach each other and interact [Javornik2022].

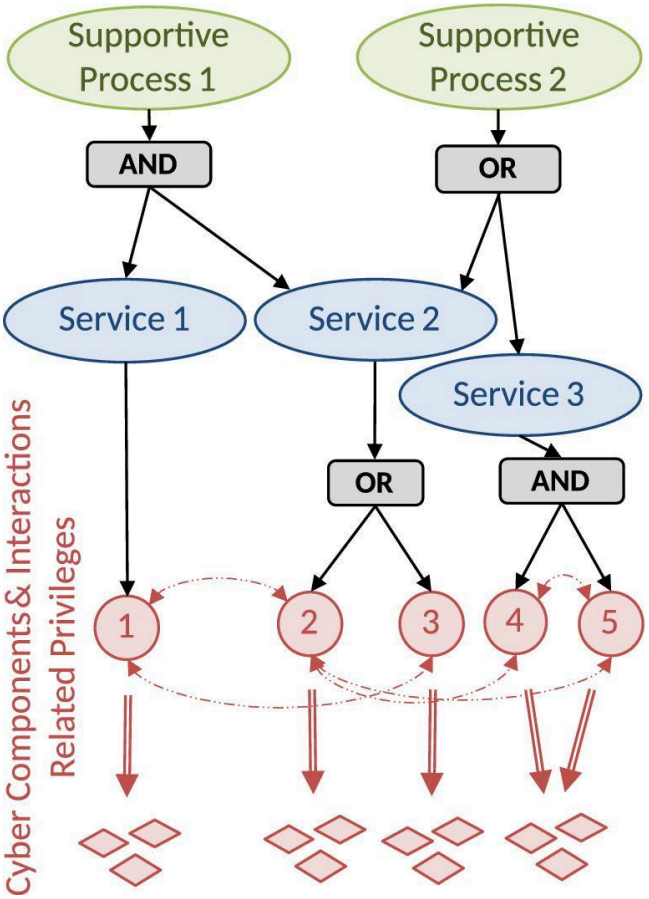


Figure 1: Mission decomposition model [Javornik2022].

An example of a mission decomposition model and its entities can be found in Figure 1. Mission-supportive processes are drawn in green, IT services in blue, and cyber components and their associated privileges in red. Full arrows and AND/OR nodes in the graphical structure visualize the dependencies between the supportive components and the logic that determines satisfying mission configurations. AND/OR trees can be more complex than just one node. Processes can share services, while services may share components. The dashed arrows between cyber components represent open communication channels when the component is used in a mission configuration. The red diamonds below the components represent the components score in terms of confidentiality, integrity, and availability (CIA) - see the related works [Javornik2019. Javornik2022, Husak2022] for more details.

Funded by
the European Union

The model was updated to allow computation of numerical scores for cybersecurity posture in the future. For this purpose, it is necessary to genuinely express criticality of missions. We allow two options of denoting how critical a mission is. The first one is to directly specify overall criticality of a whole mission ranging from 1 to 10. Number 10 is related to the most critical mission which would cause a catastrophic impact to an organization when not working properly. On the contrary, number 1 expresses a limited adverse impact to the organization. Numbers in the middle of the range indicate a serious adverse impact.

The second option uses confidentiality, integrity, and availability requirements for the mission instead of overall criticality. Individual requirements have values from 1 to 10. Their meaning is similar to numbers used for the overall criticality. Number 10 means the most critical requirement. The organization would encounter catastrophic impact when the requirement is violated. Number 1 means a limited adverse impact and numbers in the middle of the range a serious adverse impact.

2.2 Creating Mission Representations

In order to create our own decomposition of a mission, it is necessary to identify what mission supportive processes are. Mission supportive processes can have various names according to goals of different organizations. However, when focusing on cybersecurity, we can focus on network design. According to best practices, networks should be organized into segments.

This organization into segments reveals what hosts and network services should be protected by hiding them from the Internet. Devices in one segment can freely communicate with each other, hence the segments may indicate what are mission supportive processes. For example, the server segment usually contains important servers. We can identify which of them are important and should become cyber components. IT services will directly correspond to cyber components or will aggregate multiple components that serve as replicas. For example, in the case of providing files (IT service) we could have a primary file server (cyber component) and its backup servers (cyber components). Finally, it is necessary to give a name to a mission supportive process that aggregates all IT services, e.g., "*critical servers*".

Another approach for the mission decomposition works in the opposite way. We need to consider what cyber attacks would impact our organization. Do we need to protect the availability of services? Which services? Do we store sensitive data that should not be read or modified? In other words, it is necessary to identify cyber components that should have confidentiality, integrity, and availability requirements. Consequently, we can aggregate cyber components into IT services and mission supportive processes, if some of the components are related to each other.

The process of defining mission decomposition can be explained on data from a cyber defense exercise. Details about the exercise are available in a corresponding

article [Tovarnak2020]. There were six defensive (blue teams) that protected their identical networks. Figure 1 from the referenced paper containing the network topology for team number one is the most important for understanding this example. The raw data are publicly available as a dataset[1].

Figure 1 from the paper [Tovarnak2020] shows that the network is organized into four segments according to the role of hosts. In this example, we can create a mission supportive process for each of these segments according to their roles. Figure 2 contains example decomposition of mission supportive processes for DMZ and USR segments. The mission supportive processes are denoted by green colour, IT services by blue, and supportive cyber components by red colour. The mission of *public-facing services* only requires functionality of its services. Therefore, its decomposition contains only AND nodes. Mission of *user services* requires functionality of its desktops. However, it is enough to have only one desktop of each type. Therefore, its decomposition contains OR nodes. The user services have four allowable configurations: 1) *desktop1* and *desktop3*, 2) *desktop1* and *desktop4*, 3) *desktop2* and *desktop3*, and 4) *desktop2* and *desktop4*.

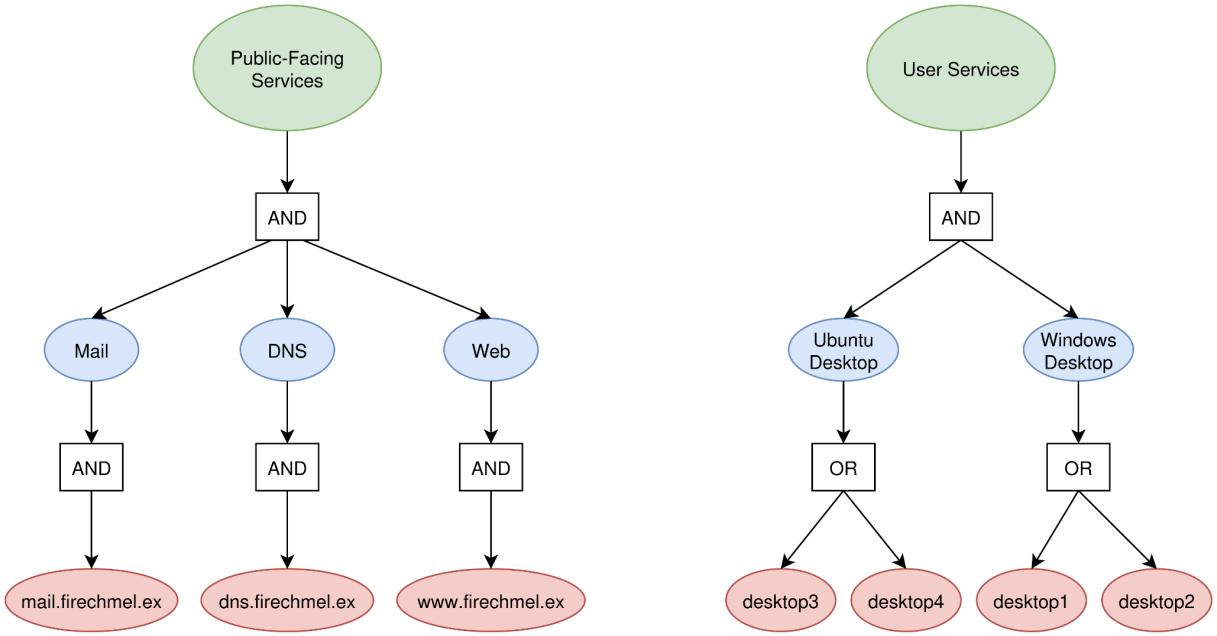


Figure 2: AND/OR tree for examples of enterprise missions.

It is possible to use a combination of OR and AND nodes to express multiple combinations of IT services that will provide functionality for a mission. An example can be found in [Javornik2019] in Figure 1. The mission supportive process of diagnostics uses one OR node that leads to two AND nodes to express that diagnostics can be achieved using local or external cyber components.

[1] https://doi.org/10.5281/zenodo.3746129

2.3 Resilmesh Implementation

The Resilmesh system implements mission modeling and mission-to-asset mapping in several components. Namely, it allows the user to specify a mission in the SACD dashboard, stores it in the ISIM database, and leverages it for risk calculations in the CSA component. Resilmesh uses automated tools to collect information on the network and cyber assets and stores the data in ISIM along with the results of vulnerability scans and other analytical tools. Certain methods can estimate the criticality of each cyber asset, i.e., how important it is for the network based on network traffic or topology analysis, and detect functional dependencies using the detection of frequent, repeated network communication patterns. Even though such methods can estimate which devices are important and how they depend on each other, these methods cannot compete with a well thought-out definition of a mission.

Designing the model itself is a delicate task, but implementing it is relatively straightforward. Mission tree structures can be described in a common JSON format and stored in any document database or attached to existing data, such as in case of ISIM. Nevertheless, from the user perspective, it is very difficult to write down a mission model, especially for non-technical users. Thus, Resilmesh implements a graphical mission editor in its SACD dashboard to facilitate this task. The editor allows for creating or editing missions, suggests elements to add, looks up assets to map to, and checks for the validity of the model. An example can be seen in Figure 3. When a user is done with the model, the model is exported into a JSON file and stored in ISIM along with the data on assets.

Once a mission is defined, Resilmesh may use the descriptions for personalizing the risk and impact assessment for the local environment. For example, a workflow in the CSA component includes the analysis of missions into more precise estimation of host criticality. The degree and betweenness centrality measures are provided by other Resilmesh components and derived from measurements by active network scanning and network traffic monitoring. The computation of final criticalities is based on normalization and multiplication of intermediate results. First, the degree centrality is normalized with respect to the count of edges and the betweenness centrality with respect to minimum and maximum betweenness centrality. The normalized values are real numbers from 1 to 10. Consequently, we compute the final criticality for a network node as a product of normalized degree and betweenness centralities that is multiplied by mission criticality for the node. The result belongs to range from 1 to 100:

$$criticality = \left(\frac{9 \cdot degree_{norm} \cdot betweenness_{norm}}{100} + 1 \right) \cdot criticality_{mission}$$

Thus, the definition of a mission not only specifies the structure of critical infrastructure in the network, but also helps in other parts of Resilmesh. Such final criticality metrics can then be used to, for example, prioritizing vulnerabilities to patch or attacks to mitigate.

Funded by
the European Union

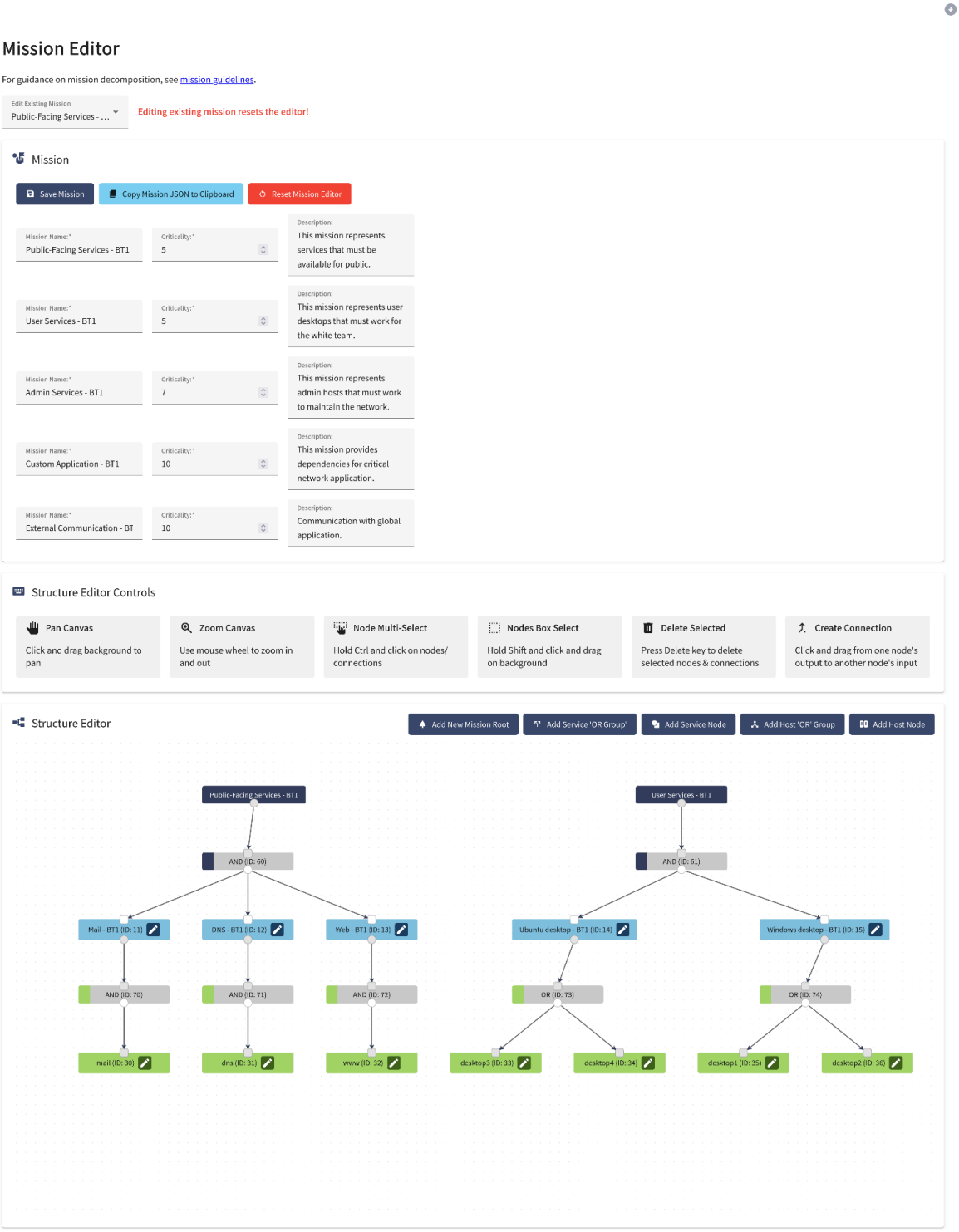


Figure 3: Mission editor that can be used for manual creation and editing of missions in the dashboard.

Funded by
the European Union

3. Related Works and Standards

Herein, we first briefly summarize related works of research, namely those introducing ways to modelling and mapping business missions to cyber assets. Subsequently, we comment on industry standards and comment on standardization efforts and possibilities of converting between models.

3.1 Related Scientific Works

The Cyber Assets, Missions, and Users (CAMUS) system [Goodall2009] provides a proof-of-concept for automatically mapping cyber assets to their associated missions and end users. This model enriches user, mission, asset, and capability entities with granular contextual data, such as organizational roles and primary workstations. Buchanan [Buchanan2012] detailed the underlying structural framework.

Other related research has focused on quantifying cyber mission impact across various domain settings. Musman et al. [Musman2011] evaluated mission impact within military scenarios by employing business process modeling notation to capture a mission's dynamic and temporal characteristics, measuring impact as degraded measures of effectiveness caused by cyber incidents. Sun et al. [Sun2015] combined a Mission-Task-Asset (MTA) map with a System Object Dependency Graph (SODG) tracking OS-level intrusion propagation, using Bayesian networks to quantify overall mission impact. Lei [Lei2015] highlighted the role of cyber situational awareness in maintaining mission continuity across attack phases using impact dependency graphs. Similarly, Guion and Reith [Guion2017] mapped missions to a cyber terrain encompassing systems, software, data, processes, and personas to evaluate strategic advantages for attackers and defenders. Shifting focus toward risk assessment, Silva and Jacob [Silva2018] proposed a mission-centric methodology that models enterprise relationships and risk metrics before assessing threat impact against mission viability.

The Resilmesh approach draws direct inspiration from the foundational research of Gabriel Jakobson and colleagues. Lewis et al. [Lewis2008] introduced a reference model for impact assessment and attack projection by treating mission evaluation as a constraint satisfaction problem within a constraint network, utilizing certainty factors theory alongside probabilistic reasoning. Later studies introduced conceptual graphs to model attack-to-mission impacts [Jakobson2011mission] and project potential security scenarios [Jakobson2011extending]. These models evaluate a cyber terrain's functional capacity to support a mission, which degrades during cyber attacks. Jakobson further detailed principles and architectures for transitioning from IT-centric to mission-centric defense [Jakobson2013], summarizing these concepts in a comprehensive chapter on mission resilience technologies [Jakobson2014].

More recently, cyber resilience has emerged as a central paradigm aligning cybersecurity with operational business continuity. Huang et al. [Huang2022]

proposed an automated response mechanism that optimizes security reconfigurations to minimize attack risks while preserving critical functionality based on system state and attacker footprint. Hutschenreuter et al. [Hutschenreuter2021] developed a resilience framework combining attack detection with ontologies and inference systems to automate detection, response, and recovery. From an analytical perspective, Zhang and Malaccaria [Zhang2021] formulated a mathematical model pairing Markov chains with attack graphs to determine optimal security control portfolios against strategic attackers over time.

Building upon these foundations, the Resilmesh approach expands the mission decomposition model introduced in our earlier work [Lewis2008, Jakobson2014, Javornik2019]. The model utilizes the AND/OR logical representations grounded in constraint satisfaction problems. However, unlike prior work that evaluates continuous mission capacity, our model treats functional constraint fulfillment as a binary condition. This underlying logic enables the identification and selection of the most resilient configuration among all feasible options - deriving a Bayesian network of associated privileges across critical targets and probable attacker positions to evaluate total system resilience.

3.2 Industry Standards

Since mission modeling and mapping was mostly addressed by researchers and only recently emerged as a tool used by practitioners, there are not yet many outstanding standards apart from SPDX discussed further. Nevertheless, there are emerging standards that are filling both the research gap and industrial needs, with SBOM being the prime example and leader in standardization.

A **Software Bill of Materials (SBOM)** is a structured, machine-readable inventory of software components, dependencies, and hierarchical relationships within an application or system. Similar to an ingredient list in physical manufacturing, SBOMs enable organizations to track software provenance, manage supply chain vulnerabilities, and audit compliance. Standardizing this metadata relies on three primary data exchange formats:

- **CycloneDX:** Maintained by the OWASP Foundation, CycloneDX is a lightweight specification designed specifically for application security, vulnerability identification, and supply chain analysis. It supports representations of software, hardware (HBOM), and services (SaaS-BOM), utilizing a dependency graph structure that explicitly captures component relationships.
- **SPDX (Software Package Data Exchange):** An ISO/IEC standard (ISO/IEC 5962:2021) managed by the Linux Foundation. SPDX was originally developed for open-source license compliance and copyright tracking, but has expanded into a comprehensive specification for software composition analysis, security vulnerability mapping, and build metadata tracking.
- **SWID (Software Identification) Tags:** Defined by ISO/IEC 19770-2:2015 and heavily adopted by NIST, SWID tags are XML-based records installed directly alongside software binaries on an endpoint. Unlike static source-level SBOM

documents, SWID tags primarily serve device management and enterprise IT asset discovery, tracking installed software states across operating environments.

3.3 Harmonization of Resilmesh with Industry and NIS2

The European Union's NIS2 Directive (Directive 2022/2555) mandates elevated cybersecurity risk-management measures and strict reporting requirements for critical and essential entities across Europe. A central pillar of NIS2 (specifically Article 21) concerns supply chain security, requiring regulated organizations to address vulnerabilities inherent in vendor relationships and third-party software products.

Standardized inventory models like CycloneDX and SPDX serve as operational enablers for meeting NIS2 compliance requirements in three key ways.

- **Supply Chain Risk Assessments:** Standardized SBOMs provide the granular transparency necessary to evaluate third-party software dependencies, enabling entities to systematically audit critical vendors for known vulnerabilities (CVEs) before integration.
- **Rapid Incident Response & Vulnerability Management:** NIS2 establishes tight incident notification timelines (e.g., initial warning within 24 hours). When novel zero-day vulnerabilities emerge (such as Log4Shell), automated parsing of SPDX and CycloneDX documents allows security operations teams to immediately determine whether affected libraries exist in their software supply chain without conducting manual code audits.
- **Bridge to Mission-Centric Resilience:** While SBOMs enumerate what components exist in the infrastructure, linking these software inventories to functional dependency trees (such as mission models) allows organizations to assess the operational impact of a supply chain compromise—aligning software asset management directly with NIS2's mandate for business continuity and risk mitigation.

The Resilmesh framework natively aligns with the strategic requirements of the NIS2 Directive by extending static supply chain visibility into dynamic, mission-centric resilience management. While NIS2 mandates that critical entities manage supply chain risks and maintain operational continuity, traditional Software Bill of Materials (SBOM) formats like CycloneDX provide an inventory of software components and their raw technical dependencies. Both Resilmesh and CycloneDX bridge this gap by ingesting the asset lists and dependency graphs directly into their mission models. This harmonization maps low-level software components and vendor vulnerabilities directly to high-level operational missions, allowing organizations to automatically evaluate how a supply chain compromise impacts core capabilities and business continuity as required by NIS2 Article 21.

Funded by
the European Union

4. Conclusion

This paper presented a mission-centric approach to cyber resilience, transitioning security evaluation from asset-level vulnerability tracking to high-level operational assurance. By illustrating the implementation of an advanced mission-decomposition framework within the **Resilmesh** platform [Bernabe2025], we demonstrated how **AND/OR logical constraints** [Javornik2019, Javornik2022] model functional dependencies, reveal single points of failure, and enable the automated selection of optimal resilience configurations during active cyber incidents.

Furthermore, we examined how this mission model aligns with modern software transparency standards and regulatory mandates. Integrating **CycloneDX** Software Bills of Materials (SBOMs) into Resilmesh bridges static supply chain component visibility with dynamic mission impact assessment. This combination addresses key requirements of the European Union's **NIS2 Directive** by providing critical entities with automated risk evaluation, rapid incident response capabilities, and continuous business continuity management.

References

[Bernabe2025] Bernabé, J. B., Lee, B., Husák, M., Sadlek, L., Stojanović, B., Somma, M., ... & La, V. H. (2025, June). The Resilmesh Architecture: Situation Aware Enabled Cyber Resilience for Dispersed, Heterogenous Cyber Systems. In 2025 IEEE 11th International Conference on Network Softwarization (NetSoft) (pp. 621-626). IEEE.
[Husak2022] Husák, M., Sadlek, L., Špaček, S., Laštovička, M., Javorník, M., & Komárková, J. (2022). CRUSOE: A toolset for cyber situational awareness and decision support in incident handling. Computers & Security, 115, 102609.
[Javornik2019] M. Javorník, J. Komárková, and M. Husák. "Decision Support for Mission-Centric Cyber Defence," ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security, 2019.
[Javornik2022] Javorník, M., & Husák, M. (2022). Mission-centric decision support in cybersecurity via Bayesian Privilege Attack Graph. Engineering Reports, 4(12), e12538.
[Jakobson2014] Jakobson G. Mission Resilience. Springer International Publishing; 2014:297-322.
[Tovarnak2020] D. Tovarňák, S. Špaček, and J. Vykopal. "Traffic and log data captured during a cyber defense exercise." Data in Brief, 2020.
[Goodall2009] Goodall JR, D'Amico A, Kopylec JK. Camus: automatically mapping cyber assets to missions and users. Proceedings of the Military Communications Conference, 2009. MILCOM 2009; 2009:1-7; IEEE.
[Buchanan2012] Buchanan L, Larkin M, D'Amico A. Mission assurance proof-of-concept: mapping dependencies among cyber assets, missions, and users. Proceedings of the 2012 IEEE Conference on Technologies for IEEE Homeland Security (HST); 2012:298-304; IEEE
[Musman2011] Musman S, Tanner M, Temin A, Elsaesser E, Loren L. Computing the impact of cyber attacks on complex missions. Proceedings of the 2011 IEEE International Systems Conference; 2011:46-51; IEEE.

[Sun2015] Sun X, Singhal A, Liu P. Who touched my mission: towards probabilistic mission impact assessment. Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense; 2015:21-26; ACM.
[Lei2015] Lei J. Cyber situational awareness and mission-centric resilient cyber defense. Proceedings of the 2015 4th International Conference on Computer Science and Network Technology (ICCSNT); Vol. 01, 2015:1218-1225.
[Guion2017] Guion J, Reith M. Cyber terrain mission mapping: tools and methodologies. Proceedings of the 2017 International Conference on Cyber Conflict (CyCon US); 2017:105-111; IEEE.
[Silva2018] Silva FRL, Jacob P. Mission-centric risk assessment to improve cyber situational awareness. Proceedings of the 13th International Conference on Availability, Reliability and Security; 2018:56; ACM.
[Lewis2008] Lewis L, Jakobson G, Buford J. Enabling cyber situation awareness, impact assessment, and situation projection. Proceedings of the MILCOM 2008 - 2008 IEEE Military Communications Conference; 2008
[Jakobson2011mission] Jakobson G. Mission cyber security situation assessment using impact dependency graphs. Proceedings of the 14th International Conference on Information Fusion; 2011:1-8; IEEE.
[Jakobson2011extending] Jakobson G. Extending situation modeling with inference of plausible future cyber situations. Proceedings of the 2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA); 2011:48-55
[Jakobson2013] Jakobson G. Mission-centricity in cyber security: architecting cyber attack resilient missions. Proceedings of the 2013 5th International Conference on Cyber Conflict (CYCON 2013); 2013.
[Huang2022] Huang Y, Huang L, Zhu Q. Reinforcement learning for feedback-enabled cyber resilience. Annu Rev Control. 2022;18.1-6.
[Hutschenreuter2021] Hutschenreuter H, Çakmakçi SD, Maeder C, Kemmerich T. Ontology-based cybersecurity and resilience framework. Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP 2021) SCITEPRESS; 2021:458-466.
[Zhang2021] Zhang Y, Malacaria P. Optimization-time analysis for cybersecurity. IEEE Transactions on Dependable and Secure Computing. 2021.