Conceptual Modeling of Cybersecurity Threats and Their Impact on Fundamental Rights

Nicolò Maunero[1,*], Andrea Bernardini[2], Mario Lezoche[3], Francesco D'Alterio[2], Federica Casarosa[4], Giovanni Comandé[4], Marina Settembre[2] and Stefano Solari[5]

[1]IMT Scuola Alti Studi Lucca, Lucca, Italy
[2]Fondazione Ugo Bordoni, Viale del Policlinico, 147, 00161, Rome, Italy
[3]University of Lorraine, CNRS, CRAN, Nancy, F-54000, France
[4]Sant'Anna School of Advanced Studies, Pisa, Italy
[5]Leonardo, Divisione Cyber & Security Solutions, Genoa, Italy

Abstract

The increasing complexity of cybersecurity threats, combined with the pervasive integration of information technologies into everyday life, calls for a rethinking of how cybersecurity risks are assessed and managed. Contemporary organizations are no longer required only to protect digital assets, services, and processes, considering not only the impact associated with their own activities, but also to account for the consequences that cybersecurity incidents may have on individuals and their fundamental rights. This shift is reinforced by the evolving European regulatory landscape, where cybersecurity obligations and fundamental rights protection increasingly intersect.

In this paper, we propose an ontology-based framework for cybersecurity risk assessment that aims to harmonize technological risk with user's necessities, moving from common privacy impacts to a more comprehensive assessment of user's fundamental rights. The proposed ontology enables the structured modeling of an organization's ICT infrastructure, including assets, services, and processes, and cybersecurity information (threats, vulnerabilities, and attacks) while providing three distinct points of view (e.g., legal entity, service provider, and final user) on impacts and consequences of identified risks. This will provide a cohesive and harmonized overview of possible consequences correlating technological risk with user's fundamental rights.

By establishing a continuous semantic chain from technological components and threat materialization to legally relevant damages, the proposed approach bridges the gap between traditional cybersecurity risk management and emerging regulatory requirements related to users' fundamental rights. The ontology provides a coherent conceptual foundation for integrated, explainable, and extensible cybersecurity risk assessment, supporting more informed decision-making across technical, organizational, and legal dimensions.

Keywords

ontology, cybersecurity risk, regulation, formalization, fundamental rights

The rapid evolution of information and communication technologies, coupled with the increasing sophistication of cyber threats, has profoundly transformed the landscape of cybersecurity risk. Digital infrastructures now support essential services across critical domains such as healthcare, finance, transportation, and public administration, making cybersecurity incidents not only a technical concern but also a societal one. As a consequence, cybersecurity risks can no longer be assessed solely in terms of system availability, data integrity, or economic loss; they must also account for their broader impacts on individuals and society.

Traditionally, organizations have focused their cybersecurity risk management efforts on protecting digital assets, services, and operational processes. Although this remains a fundamental requirement, it is becoming increasingly insufficient. Cybersecurity incidents may directly or indirectly affect end users, exposing them to harms that extend beyond privacy violations to encompass a wider range of fundamental rights, such as access to essential services, non-discrimination, safety, and autonomy.

Joint National Conference on Cybersecurity (ITASEC & SERICS 2026), February 09-13, 2026, Cagliari, IT
*Corresponding author.
nicolo.maunero@imtlucca.it (N. Maunero); abernardini@fub.it (A. Bernardini); mario.lezoche@univ-lorraine.fr (M. Lezoche); fdalterio@fub.it (F. D'Alterio); federica.casarosa@santannapisa.it (F. Casarosa); giovanni.comande@santannapisa.it (G. Comandé); msettembreo@fub.it (M. Settembre); stefano.solari@leonardo.com (S. Solari)
0000-0002-4331-1066 (N. Maunero)

This shift in perspective challenges established risk assessment methodologies, which often lack the conceptual tools to capture such human-centric consequences.

In recent years, cybersecurity regulations have undergone significant evolution, becoming increasingly pervasive in the critical sectors of the market. In Europe, various legislations have been adopted and implemented at the national level with the aim of defining and harmonizing the obligations of public and private organizations and entities in terms of cybersecurity. This has led, on the one hand, to improved requirements for critical infrastructure in terms of asset protection and risk management (NIS 1 [1] and NIS 2 [2], Cyber Resilience Act [3]), but also to an improvement in all aspects related to user rights over personal data (GDPR) [4], taking into account the introduction of new and emerging technologies (AI Act) [5]. It is precisely in this context that the need has emerged to consider the impact of technology not only on user privacy, but more generally on their fundamental rights (AI Act).

Therefore, it is becoming increasingly necessary and essential to consider the consequences of cyberattacks and incidents not only at a technical level (e.g., downtime, loss of revenue, malfunctions, and so on) but also in terms of the impact they may have on the fundamental rights of the user involved. This is an aspect that can also greatly influence the way in which an organization is required to manage risk ex ante (before the incident) and ex post (after the incident or materialization of the risk), as mitigation actions and security mechanisms implemented can have an impact on the user despite ensuring effective risk mitigation.

In this paper, we address this challenge by proposing an ontology for cybersecurity risk assessment and management that integrates conceptual modeling, threat analysis, and fundamental rights considerations within a unified semantic framework. The ontology enables the formal representation of ICT infrastructures—modeled in terms of assets, services, and processes—together with cybersecurity threats, vulnerabilities, and attacks. Crucially, it introduces multiple stakeholder perspectives, including legal entities, service providers, and end users, allowing the differentiated analysis of impacts and damages arising from cybersecurity incidents.

By explicitly modeling the relationships between technological risk factors and their consequences on users' fundamental rights, the proposed ontology aims to bridge the gap between traditional cybersecurity risk management and emerging regulatory and societal expectations. The remainder of the paper is structured as follows. Section 1 reviews the main standards, frameworks, and regulatory concepts that inform the proposed approach. Section 2 discusses related work on ontology-based cybersecurity risk assessment. Section 3 presents the core contribution of this work, introducing the proposed approach and detailing the ontology and its conceptual domains. Finally, Section 4 concludes the paper and outlines directions for future work.

1. Background

The development of a cybersecurity risk assessment ontology that explicitly integrates threat analysis and fundamental rights considerations requires grounding in both established technical standards and emerging regulatory and legal frameworks. Cybersecurity risk does not exist in a conceptual vacuum: it is shaped by internationally recognized methodologies for risk management, as well as by evolving legal obligations that increasingly emphasize the protection of individuals and their rights. For this reason, the proposed ontology has been informed by a careful analysis of reference standards and frameworks that collectively define the current state of practice and regulation.

On the technical side, international standards such as those developed by ISO/IEC and methodological frameworks proposed by ENISA provide a consolidated vocabulary and conceptual structure for modeling ICT systems, cybersecurity risks, and risk management processes. These standards play a crucial role in ensuring consistency, interoperability, and acceptability of risk assessment practices across organizations and sectors. They also introduce key concepts—such as assets, processes, services, stakeholders, and consequences—that form the backbone of many cybersecurity risk management approaches.

At the same time, recent regulatory developments, particularly within the European Union, have

expanded the scope of cybersecurity risk assessment beyond purely technical and organizational concerns. Instruments such as the GDPR and the Artificial Intelligence Act highlight the need to consider how technological risks may affect individuals' fundamental rights, thus introducing new requirements for impact assessment, accountability, and transparency. In this context, the notion of Fundamental Rights Impact Assessment emerges as a critical complement to traditional cybersecurity risk analysis, yet remains insufficiently integrated into existing technical frameworks.

This section provides the background necessary to position the proposed ontology at the intersection of these two dimensions. Section 1.1 reviews the main reference standards and frameworks that inform the modeling of technological systems, cybersecurity risks, and risk management actions, with particular attention to how they conceptualize stakeholders and consequences. Section 1.1.2 introduces the concept of Fundamental Rights Impact Assessment, outlining its relevance for cybersecurity and motivating the need for a unified conceptual framework capable of linking threat analysis with legally relevant notions of damage and harm.

Together, these background elements establish the conceptual and regulatory foundations upon which the ontology presented in Section 3 is built, and clarify the rationale for integrating technical, organizational, and human-centric perspectives within a single semantic model.

1.1. Reference Standards and Frameworks

This section will briefly present the two main reference standards and frameworks considered for modeling concepts in the proposed ontology. We will not describe in detail the presented standards and frameworks, but it is important to highlight the main points that were taken as reference for designing the proposed ontology. It should also be considered that, in the effort made to formalize knowledge, particular care has been taken to refer to commonly shared concepts and relations used in cybersecurity risk management.

1.1.1. ISO/IEC

The 27000 series published by ISO/IEC [6] is one of the de facto reference standards for implementing an effective information security management system. The documents in the series provide guidelines and requirements for establishing, implementing, maintaining, and continually improving an information security management system.

Several concepts for the design of the ontology presented in Chapter 3.2 have been extrapolated from this series of standards. Given the need to provide an interoperable tool for the representation and modeling of concepts and relationships that are fundamental to risk assessment and management, reference to standards such as those of ISO, which are widely used as references for frameworks and regulations, becomes essential.

The main points of interest that have been extrapolated refer mainly to ISO/IEC 27005 [7], but are nevertheless included throughout the series. This document describes in more detail, and mainly focuses on, the risk management process, identifying its main elements, the stakeholders involved, and what activities or information are necessary for the implementation of the entire process.

First, we have the concept of *Risk Owner*, which represents those entities within the organization that must be accountable and have the authority to properly manage the identified risk; and the concept of *interested parties*, which generally represents all persons who perform or are involved in the process of information security risk management.

These fundamental elements have been used in the proposed ontology for modeling the user class and the relationships they have with infrastructure elements, risks, and their consequences.

Another interesting aspect presented in ISO/IEC 27005 is the definition of consequence criteria. Consequences are directly or indirectly affected by the preservation or loss of confidentiality, integrity, and availability. Several categories are identified, including both the consequences of an impact on the technological infrastructure and those that could affect the end user. From this list, the impact categories in the proposed ontology have been extrapolated and then assigned to the resulting damages.

1.1.2. ENISA

In Europe, ENISA developed a risk assessment framework. The document "Methodology for Sectoral Cybersecurity Assessments" (SCSA Methodology) [8] was published in 2021, following and building upon the European Cybersecurity Act (CSA) [9]. The proposed methodology has the objective of linking the risk assessment process with the CSA requirements in terms of cybersecurity certifications; providing a methodology that allows interpreting the result of the assessment with the certification process an organization may undergo following ISO 27000 [6] and ISO 15408 [8].

The methodology first presents the concept of an ICT system as an ICT service that is supported by ICT products and ICT processes, and provides a distinction between two layers of an ICT system:

- ICT Infrastructure: which serves several markets, applications and end-users services. For example, an ICT infrastructure can be cloud services or mobile networks; an infrastructure that provides some sort of service to the sectoral ICT system it supports.
- Sectoral ICT Systems: which include all functions that are specific to the delivery of service to a particular market sector targeted at end-users. Usually, Sectoral ICT systems rely on ICT infrastructure services for specific functions.

Moreover, the methodology identifies the composition, in terms of architecture and interaction among various components, of an ICT system as the basis for identifying possible threats and security requirements.

The evaluation of cybersecurity risks depends on the sectoral stakeholders' objectives and the relevant business processes that might be impacted by security events. The identification of these requirements is done by focusing on the *supporting assets* of the analyzed system. These two different viewpoints are bound together in the SCSA Methodology through the concepts of *primary information assets* and *primary functional assets*. *Primary assets* are information and functions that are relevant to the business goal; while *supporting assets* are those that support the primary assets and play a key role in the system. *Information assets* are basically data, where *functional assets* are software and hardware that allow activities to be carried out.

Following the definition provided by the SCSA methodology, in the proposed ontology (see Section 3.2) we adopted a similar approach in defining the high level concepts necessary to represent the technological domain of the target infrastructure and the centerpieces upon which risk is evaluated.

1.2. Fundamental Rights Impact Assessment

The concept of Fundamental Rights Impact Assessment (FRIA) originates in legal and regulatory contexts as a structured process aimed at identifying, evaluating, and mitigating the potential adverse effects of technological systems on individuals' fundamental rights. It relies on the pre-existing Data Protection Impact Assessment, included in Article 35 of the General Data Protection Regulation (GDPR), and the Human Rights Impact Assessment, a due diligence practice adopted by both public and private actors [10]. Unlike traditional risk assessments, which primarily focus on technical failures, economic losses, or organizational disruptions, FRIA explicitly centers on the protection of rights enshrined in constitutional frameworks, international conventions, and, in the European context, the Charter of Fundamental Rights of the European Union.

In recent years, FRIA has gained particular relevance in the domain of digital technologies due to the increasing deployment of complex, data-driven, and automated systems. The adoption of the GDPR introduced the obligation for specific types of data processing of a Data Protection Impact Assessment (DPIA), which focuses specifically on risks to privacy and data protection rights. However, subsequent regulatory developments, most notably the Artificial Intelligence Act, extend this logic beyond data protection and privacy, requiring organizations to assess risks to a broader set of fundamental rights, including i.e., non-discrimination, human dignity, access to essential services, safety, and effective remedy. The structure of the impact assessment, however, has remained unchanged: it is based on an ex ante approach that requires a rights-based risk assessment, which should be expert-based; moreover,

the evaluation is not limited to one phase, but rather it is an iterative structure following the lifecycle of the product or service.

From a legal perspective, a fundamental rights impact assessment aims to determine whether the deployment or operation of a technological system may negatively affect the rights and freedoms of individuals. However, so far, the studies carried out addressed emerging risks with limited attention to the subsequent quantification of harm [11, 12].

The current analysis aims to extend the research to the connection between the ‘impact" on fundamental rights and the potential harm that is legally relevant. This harm is not limited to abstract (harm-event) or speculative risks, but is evaluated in relation to concrete adverse effects on identified rights holders (harm-consequence) [13]. Importantly, legal analysis distinguishes between potential adverse effects and actual harm, defined as damage. Damage, in this sense, denotes a legally cognizable injury that may give rise to obligations of mitigation or liability (through economic compensation).

This distinction is essential for the conceptual modeling proposed in this work. In legal doctrine, damage is generally understood as the materialization of harm beyond a tolerable threshold [14], producing consequences that are actionable under applicable legal frameworks. Such damages may be material (e.g., financial loss, service interruption), immaterial (e.g., reputational harm, loss of autonomy), or mixed, and they may affect different categories of subjects, including organizations and individuals. Crucially, damages related to fundamental rights often concern end users who have no direct control over the technological systems that generate the risk.

From a computer science and cybersecurity perspective, existing risk assessment methodologies rarely make this distinction explicit. Impacts are often treated as direct consequences of incidents, quantified in technical or economic terms, without a formal separation between potential effects assessed ex ante and legally relevant damages observed ex post. This gap makes it difficult to align technical risk analysis with regulatory requirements related to fundamental rights.

The approach adopted in this paper addresses this limitation by explicitly incorporating the legal logic of FRIA into the conceptual model. In particular, it distinguishes between impact, understood as the potential or observed consequence of a cybersecurity incident resulting from the degradation of confidentiality, integrity, or availability, and damage, understood as the realization of such impact once it exceeds a defined offensiveness threshold. This threshold reflects legal, organizational, and societal criteria that determine when an impact becomes unacceptable and legally actionable.

By introducing this threshold-based relationship, the model allows cybersecurity impacts to be assessed in a manner that is compatible with legal reasoning while remaining amenable to formalization and computational treatment. Impacts can be identified and evaluated during risk analysis, whereas damages represent the subset of impacts that trigger legal relevance, accountability, and possible compensation. This distinction is particularly important in contexts where cybersecurity incidents affect fundamental rights indirectly, for example through the disruption of essential services, discriminatory outcomes, or constraints on individual autonomy.

In summary, Fundamental Rights Impact Assessment provides the legal and conceptual foundation for extending cybersecurity risk assessment beyond traditional technical boundaries. By integrating FRIA concepts into an ontology-based framework, this work creates a bridge between cybersecurity engineering and legal compliance, enabling a unified representation of threats, impacts, and damages that supports both technical decision-making and fundamental rights protection.

2. Related Work

Ontologies born for modeling and formalizing knowledge, can be applied to different knowledge domains and for different applications. They can create a common language and a knowledge-base that can be shared, integrated, and reused. The use of ontologies in cybersecurity has increased over the years, especially in applications related to cybersecurity risk, as a tool for knowledge formalization to foster interoperability among the different standards and regulations, for the collection and management of information from unstructured sources, and to support reasoning and inference [15].

There are some useful literature reviews that try to collect the most important cybersecurity ontology proposals. The works of Blanco et al. [16, 17] aim to identify the main features that an ontology should have to correctly and extensively represent a security domain, highlighting how there is still a lack of solutions that allow mapping and effectively represent all these features.

The work of Adach et al. [18] provides a comparison of the best general ontologies currently available. The study concluded, in line with previous works, that each ontology has conceptual gaps and, therefore, it is necessary to work to create a unified solution.

Finally, the work of Souag et al. [19] also comes to the same conclusion that there is currently too much disparity between the security requirements requested and the modeling of these in an ontology.

Several ontology-based approaches have been proposed to support different phases of the risk assessment and management process.

The *Unified Cybersecurity Ontology* [15] aims to change the approach of cybersecurity standards from a syntactic representation to a more semantic representation. To do so, a large number of existing standards and ontologies have been studied and reviewed, and the most common ones have been selected to be integrated with UCO. In particular, UCO is intended to be the semantic version of *STIX* [20] and it includes references to many external standards. Similarly, the work of Akbar et al. [21] tries to integrate semantically the different MITRE frameworks and data sources to better reason on complex attacks such as Advanced Persistence Threats (APT). However, these ontologies mainly focus on attack representation rather than the whole risk management process.

There are proposals in the literature that focus on different technological domains. The work of Mozzaquatro et al. [22] aims to provide a resource that should help drafting a big picture of information security in the Internet of Things field. The ontology greatly details IoT related technologies and devices and integrates the concept of security mechanism as a way of protecting the infrastructure. Onto-CARMEN [23] propose an ontology that leverages semantic constructs to automatically verify security requirements. The ontology focuses on cyber-physical systems (CPS) and aims to support the identification of missing requirements and understand how to improve the target system as new threats arise. In SIMON [24], instead, the authors propose an approach that focuses on the collection and categorization of cyber threat intelligence, in order to automate cybersecurity tasks in complex cyber-physical systems. The proposed ontology allows reasoning about threats, vulnerabilities, and attack vectors, and should help in identifying how to respond accordingly.

Oliveira et al. [25] introduced ROSE, an ontology for risk treatment and management that models security mechanisms and enables reasoning about appropriate mitigation strategies. Grigoriadis et al. [26] proposed an ontology to support risk-related information collection in CPS by integrating data from security knowledge bases, reports, and network monitoring systems, enriched with information about users and threat actors.

Other proposals, such as [27, 28, 29, 30], try to formalize and model possible cybersecurity solutions and mitigation that can be implemented at the technological level in order to deal with potential cyberattacks. They provide a detailed categorization of different security mechanisms and their relation with the technological stack that an organization may implement. What these proposals still lack is a description of other possible measures to manage risk outside of the sole technological solutions as well as a description of the complex influence on possible impact and damages of the solution applied ex ante or ex post the materialization of the risks.

Addressing contextual risk assessment, Riesco et al. [31] and later Sánchez-Zas [32] proposed ontologies that ingest SIEM alerts to enable near real-time risk evaluation. Detected incidents are analyzed through predefined rules to support dynamic risk management. Similarly, Arogundade et al. [33] proposed an ontology-based approach where risk is assessed using IDS alerts and historical threat data, and mitigation actions are suggested based on past responses or qualitative evaluations. Moreover, Khaleghi et al. [34] introduced a cyclic, context-aware risk model describing interactions between attackers and network components. The model determines network states—ranging from tolerable risk to successful attack—based on risk levels computed from data collected by network sensors.

Recently, some proposals [35, 36, 37, 38] tried to address the fundamental right impact assessment introduced by the AI act through the formalization of an ontology. These proposals aimed to model

the requirements and the information process required to support compliance with the regulation. Being specifically focused on the AI act, these proposals do not integrate other aspects of the general cybersecurity risk assessment and management process.

In general, proposals in the literature tend to focus on specific technological domains, aspects of the cybersecurity management process, and tasks to support. They can be difficult to abstract and integrate with other proposals and apply in different contexts. Moreover, there are only a few approaches that try to address the cybersecurity risk management from both the technological point of view and the legal requirements introduced by regulations and laws, as usually these two worlds are kept rather separated.

3. Contribution

The contribution of this work lies in the definition of an ontology-driven approach for cybersecurity risk assessment that explicitly connects technological risk factors with their consequences on users' fundamental rights. Unlike traditional risk models that remain confined to technical or organizational dimensions, the proposed framework establishes a continuous semantic chain that starts from the structure of the ICT system, traverses cybersecurity threats and vulnerabilities, and culminates in legally relevant impacts and damages affecting different categories of users.

This section first introduces the overall approach and its rationale, as illustrated in Figure 1, and then details how this approach is concretized through a structured ontology whose components are semantically interconnected and mutually dependent.

3.1. Proposed Approach

The proposed approach aims to model cybersecurity risk as a socio-technical and legally relevant phenomenon, rather than as a purely technical metric. To achieve this, the proposed solution establishes a structured semantic chain that connects technological system components to cybersecurity events, their consequences, and their differentiated impacts on multiple categories of users. Figure 1 provides a high-level overview of this chain and serves as a conceptual guide for the approach.

At the foundation of the approach lies the technological domain, which represents the ICT system of an organization through assets, services, and processes. These elements define both the operational capabilities of the organization and the potential targets of cybersecurity incidents. However, technological elements are not considered in isolation: their security relevance emerges only when they are evaluated with respect to the fundamental security properties defined by the CIA triad—confidentiality, integrity, and availability.

Cybersecurity events are modeled as the result of interactions between vulnerabilities, threats, and attacks acting upon technological elements, with the consequence of CIA degradation. This degradation constitutes the pivotal transition point in the model. It translates technical compromise into impact, which represents the immediate consequences of the cybersecurity event. Impacts are contextual: their severity depends not only on the extent of the CIA degradation but also on the role of the affected element within the organization and the environment in which it operates.

Impacts do not necessarily translate into damages. The proposed approach explicitly distinguishes between the two by introducing a threshold-based relationship. An impact results in damage only when it exceeds a defined threshold of offensiveness, which reflects legal, organizational, or societal relevance. This distinction is essential to align cybersecurity risk assessment with legal notions of harm, particularly in the context of fundamental rights impact assessment.

Risk is then conceptualized as an emergent property resulting from the combination of impact and probability. Probability captures the likelihood that a threat will manifest through the exploitation of a vulnerability, resulting in the generation of an impact, adjusted for contextual factors such as exposure, attacker capability, and existing controls. Risk, therefore, synthesizes both the severity of potential consequences and their likelihood of occurrence.

Two transversal dimensions interact with this entire chain. The first is the user's dimension, which introduces multiple perspectives on risk and damage. The same cybersecurity event may have different implications for a legal entity, a service provider, or an end user, particularly when fundamental rights are involved. The second is the risk management dimension, which encompasses remedial actions applied both ex ante and ex post. These actions may alter vulnerabilities, reduce probabilities, mitigate impacts, or limit damages, thereby dynamically reshaping the risk profile.

By explicitly modeling these concepts and their relationships, the proposed approach bridges technological cybersecurity assessment with legal and human-centric considerations. It provides a unified conceptual foundation for reasoning about how cyber incidents originate, how they propagate through technical systems, and how they ultimately affect organizations and individuals.

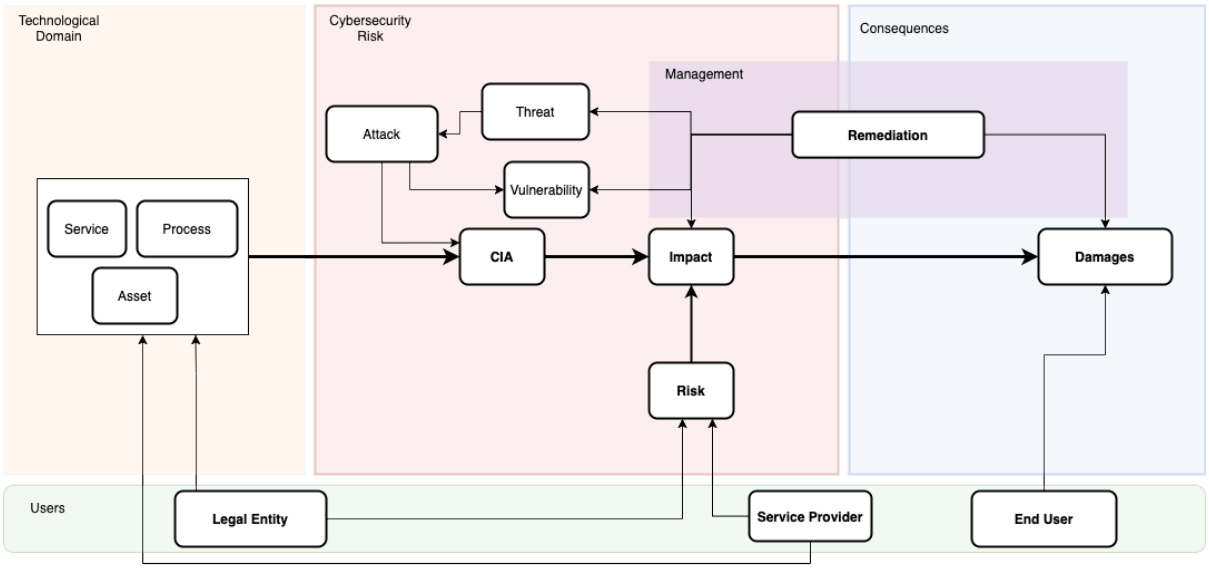

Figure 1: general overview of the proposed approach

An example of the advantages of the proposed approach can be understood by considering a possible cyberattack in the healthcare context. Consider, for example, ransomware that targets IT systems, rendering surgical IT tools unusable for a certain period of time, without which a medical team cannot operate properly. Looking at the ICT infrastructure, we see that the attack will result in downtime/service disruptions that will impact financial and reputational aspects. If, in addition to the ICT area, we also consider the possible end users (doctors and/or patients), we will be able to understand and correlate how a certain type of technological impact can affect the fundamental rights of patients (e.g., right to health) and, based on the severity of the impact, what the possible resulting damages are.

3.2. Proposed Ontology

In order to operationalize the conceptual approach described in Section 3.1, we introduce an ontology specifically designed to support a comprehensive and human-centric cybersecurity risk assessment. The ontology provides a formal and structured representation of the elements involved in the cybersecurity risk lifecycle, enabling the explicit modeling of how technological vulnerabilities and threats propagate through ICT systems and ultimately produce impacts and damages affecting different categories of users, including end users and their fundamental rights.

The ontology has been designed with two primary objectives. First, it aims to ensure conceptual coherence and interoperability with established cybersecurity standards and frameworks, such as ISO/IEC 27000, ISO/IEC 27005, ISO 9000, and ENISA methodologies. Second, it seeks to overcome the traditional fragmentation between technical risk assessment and legal or human-centric evaluations by embedding legal notions of impact and damage directly into the same semantic structure used to represent technological risk.

From a structural perspective, the ontology mirrors the causal and semantic chain illustrated in Figure 1 and introduced in Section 3.1. Rather than presenting isolated concepts, the ontology is organized into a set of interconnected conceptual domains, each of which captures a specific aspect of cybersecurity risk while remaining tightly linked to the others. This organization allows reasoning processes to traverse the entire chain, from the description of the ICT system to the assessment of consequences and remedial actions.

More specifically, the ontology is articulated into five main conceptual domains. The technological domain, detailed in Section 3.2.1, formalizes the ICT system under analysis by modeling assets, services, and processes, which constitute the primary targets and enablers of cybersecurity incidents. This domain provides the structural foundation upon which all subsequent risk-related concepts are anchored.

Building upon this foundation, the cybersecurity risk domain, presented in Section 3.2.2, captures the mechanisms through which technological elements are exposed to risk. It models vulnerabilities, threats, and attacks, their effects on the confidentiality, integrity, and availability of assets, services, and processes, and the resulting impacts and probabilities that together define risk.

The risk management domain, discussed in Section 3.2.3, introduces the actions through which organizations can influence the evolution of risk. By distinguishing between preventive, corrective, and corrective actions in accordance with international standards, this domain enables the modeling of both ex-ante and ex-post interventions and their effects on vulnerabilities, impacts, and damages.

The consequences domain, described in Section 3.2.4, formalizes the transition from technical impact to legally and socially relevant damages. This domain explicitly distinguishes between potential impacts assessed during risk analysis and actual damages that materialize when defined thresholds are exceeded, thereby aligning cybersecurity risk assessment with legal reasoning and fundamental rights considerations.

Finally, the user's domain, presented in Section 3.2.5, introduces multiple stakeholder perspectives, including legal entities, service providers, system users, end users, and threat actors. By associating impacts and damages with different user roles, the ontology captures the fact that the same cybersecurity event may have heterogeneous consequences depending on the actor involved.

Taken together, these five domains constitute a unified ontological framework that bridges technological, organizational, and legal dimensions of cybersecurity risk. The following subsections detail each domain and its internal structure, while emphasizing the semantic relationships that enable integrated reasoning across the entire risk assessment process.

3.2.1. Technological domain

Concepts: *Asset*, *Service*, *Process*.

The technological domain constitutes the structural foundation of the proposed ontology and represents the entry point for cybersecurity risk analysis. It formalizes the ICT system under assessment through three core and interdependent concepts: *Asset*, *Service*, and *Process*. These concepts are derived from widely adopted standards and frameworks, notably ISO/IEC 27000 and ENISA methodologies, and collectively describe what an organization owns, provides, and operates.

Assets represent resources of value for the organization and encompass both tangible and intangible elements, such as hardware devices, software components, datasets, communication infrastructure, and digital identities. Assets are the primary carriers of information and functionality and are therefore natural targets for cybersecurity threats. Within the ontology, assets are associated with ownership and responsibility relations, typically linked to a Legal Entity User, enabling accountability and governance considerations.

Services represent the functional capabilities delivered by the organization, either internally or externally, to support business objectives or provide value to end users. Services rely on one or more assets for their operation and may themselves be composed of sub-services, reflecting modern service-oriented and cloud-based architectures. The ontology explicitly models service composition and dependency relationships to capture cascading effects in the case of service disruption.

Processes describe the operational workflows through which assets and services are orchestrated to achieve organizational goals. Processes formalize sequences of activities, roles, and interactions, and provide the contextual layer that connects technological elements to organizational functions. A single process may involve multiple services and assets, while a service may support several processes.

These three concepts are tightly interconnected: assets enable services, services execute or support processes, and processes operationalize services through assets. Importantly, each of these technological elements is semantically linked to the *CIA* triad, establishing the foundation for subsequent cybersecurity risk analysis. The *ServiceProvider* manages a *service*, while the *Legal Entity User* possesses an *asset*.

3.2.2. Cybersecurity Risk

Concepts: *Risk*, *Threat*, *Attack*, *Vulnerability*, *CIA*, *Impact*, *Probability*.

The security dimension is defined by the *CIA* triad: *Confidentiality*, *Integrity*, and *Availability*. Each asset, service, or process should be evaluated according to these fundamental security properties. *Confidentiality* ensures that information is accessible only to authorized individuals, *Integrity* guarantees that data remains accurate, complete, and unaltered except through authorized means, and *Availability* ensures that resources remain accessible to legitimate users when required. These properties represent practical attributes that require ongoing measurement and protection for every component within the central triad. Then, *Vulnerabilities* represent specific instances of weaknesses in the implementation or instantiation of assets, services, and processes that can be exploited, leading to potential compromise; *Threats*, in turn, refer to the possibility of adverse events, typically initiated by threat actors, defining motivations, capabilities, and opportunities which can make such exploitation process successful. *Attacks* are specific actions that allow the exploitation of these vulnerabilities using technical or procedural methods. *Probability* quantifies the likelihood that a threat will result in a successful attack, taking into account target attractiveness, required sophistication, and the effectiveness of existing controls. *Impact* assesses the multidimensional consequences of an incident across five severity levels of damage, encompassing financial, operational, reputational, regulatory, and fundamental rights effects. *Risk* is derived from the combination of probability and impact, representing the anticipated harm that informs security decisions and investment prioritization [6]. This conceptual framework outlines the progression from potential vulnerability, through the concretization of a threat and the consequent exploitation, followed by the realization of damage (impact) as weighted by probability.

3.2.3. Risk Management

Concepts: *RemedialAction*, further specialized in *RiskTreatmentAction* (ISO27000); *CorrectiveAction* (ISO 9000), *CorrectionAction* (ISO 9000).

The risk management framework is structured around *RemedialAction*, which includes all organizational measures designed to address identified risks and is divided into three distinct action types.

RiskTreatmentAction (ISO 27000) refers to ex-ante preventive mitigation implemented before incidents, targeting four dimensions: vulnerabilities through security controls and system hardening, impact through business continuity and backup capabilities, threats through deterrence and threat intelligence, and probability through detection and monitoring systems. These proactive measures employ four strategies: risk avoidance, reduction, transfer, or acceptance, determined by cost-benefit analysis and the organization's risk appetite.

CorrectiveAction (ISO 9000) involves ex-post reactive remediation conducted after incidents, addressing the root causes of vulnerabilities, threats, and damages to prevent recurrence through systematic investigation, process improvement, and control enhancement.

CorrectionAction (ISO 9000) addresses immediate ex-post remediation to eliminate specific nonconformities in vulnerabilities, impacts, and damages, focusing on symptoms rather than root causes through rapid containment, system restoration, and compliance rectification. Collectively, these three action types establish a comprehensive risk management lifecycle that integrates strategic prevention, tactical response, and operational correction, enabling organizations to minimize risk exposure

proactively and respond effectively to incidents.

3.2.4. Consequences

Concepts: *Damages*, internally specialized in *Direct Costs*, *Indirect Costs*, *Recovery Costs*, *Regulatory Fines*, *Downtime*.

The ontology delineates a critical distinction between *Impact*, defined as potential consequences assessed during risk analysis, and *Damages*, understood as actual realized harm. These concepts are linked by a threshold relationship: damages occur only when impacts surpass specific thresholds of severity, duration, or scope, thereby necessitating organizational response, stakeholder reporting, or resource allocation for remediation.

The framework employs a five-level Damage classification (IC1-IC5), ranging from minor damages manageable within operational tolerances to existential damages threatening organizational survival, as well as specializing it into multiple categories: *Direct Costs, Indirect Costs, Recovery Costs, Regulatory Fines, Downtime*.

The threshold relationship between *Impact* and *Damages* recognizes that not all assessed impacts materialize into actual damages due to successful prevention, detection, or mitigation. This threshold is influenced by organizational context, risk appetite, and regulatory requirements, and it remains dynamic based on the speed and effectiveness of the response.

3.2.5. Users

Concepts: *Legal Entity User*, *Service Provider*, *End User*, *System User*, *Threat Actor*

A *Legal Entity User* refers to organizational roles and corporate entities that interact with systems in a formal, legally accountable capacity, bearing responsibility for compliance, governance, and contractual obligations.

A *Service Provider* refers to an external entity that delivers capabilities, infrastructure, or services to the organization, thereby creating dependencies and third-party risk.

An *End User* refers to an individual who consumes services and applications, including customers, clients, or beneficiaries.

System User represents technical operators, administrators, and IT personnel who manage infrastructure, configure systems, and maintain operational capabilities with elevated privileges and direct access to critical assets.

A *Threat Actor* refers to an adversarial user who intentionally seeks to compromise security by exploiting vulnerabilities, executing attacks, and realizing threats.

4. Conclusions

This work has presented an ontology-driven framework for cybersecurity risk assessment that explicitly integrates technical threat analysis with a human-centric perspective grounded in fundamental rights protection. Moving beyond traditional approaches that primarily focus on assets, vulnerabilities, and economic losses, the proposed framework establishes a unified conceptual model capable of capturing how cybersecurity incidents propagate from technological components to legally and socially relevant consequences affecting different categories of users.

The core contribution of this paper lies in the definition of a structured semantic chain that connects ICT assets, services, and processes with threats, vulnerabilities, and attacks, and subsequently links their effects on confidentiality, integrity, and availability to impacts and damages. By explicitly distinguishing between impact and damage through a threshold-based relationship, the proposed ontology aligns cybersecurity risk assessment with legal notions of harm and accountability. This distinction is particularly relevant in light of emerging European regulations, such as the AI Act, which require organizations to assess and mitigate risks to individuals' fundamental rights.

Another key aspect of the proposed approach is the explicit modeling of multiple stakeholder perspectives, including legal entities, service providers, system users, and end users. This multi-perspective view acknowledges that the same cybersecurity incident may generate heterogeneous consequences depending on the actor involved, and it enables a more nuanced and transparent analysis of responsibility, risk ownership, and user impact. In doing so, the ontology provides a conceptual bridge between technical cybersecurity practices and regulatory compliance obligations.

From a methodological standpoint, the ontology has been designed to ensure conceptual coherence and interoperability with widely adopted standards and frameworks, such as ISO/IEC 27000, ISO/IEC 27005, ISO 9000, and ENISA methodologies. This alignment supports its adoption as a foundational model for integrated cybersecurity risk assessment and facilitates its extension toward automated reasoning, decision support, and explainable risk analysis.

Future work will focus on several complementary directions. First, the ontology will be further refined and instantiated through real-world case studies in different application domains, with particular attention to critical infrastructures and services with high societal impact. Second, the integration of dynamic data sources, such as security monitoring systems and incident reports, will be investigated to support near real-time risk assessment and adaptive risk management. Finally, the alignment of the proposed ontology with emerging fundamental rights impact assessment frameworks will be explored in greater depth, with the objective of supporting organizations in meeting both cybersecurity and regulatory requirements in a coherent and systematic manner.

Overall, this work provides a conceptual and formal foundation for a more comprehensive, explainable, and human-centric approach to cybersecurity risk assessment, contributing to the ongoing effort to reconcile technological innovation with the protection of fundamental rights.

Acknowledgments

This work was partially supported by the project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU.

Declaration on Generative AI

During the preparation of this work, the authors used Grammarly solely for grammar checking, spelling correction, and phrasing refinement to enhance readability. After using this tool, the authors thoroughly reviewed and edited all content and take full responsibility for the accuracy and integrity of the publication.

References

[1] Directive (eu) 2016/1148 of the european parliament and of the council of 6 july 2016 concerning measures for a high common level of security of network and information systems across the union, Available at https://eur-lex.europa.eu/eli/dir/2016/1148/oj, 2016.

[2] ENISA, Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, Available at https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new, 2023. Accessed: 2025-12-17.

[3] Regulation (eu) 2024/2847 of the european parliament and of the council of 23 october 2024 on horizontal cybersecurity requirements for products with digital elements and amending regulations (eu) no 168/2013 and (eu) 2019/1020 and directive (eu) 2020/1828 (cyber resilience act), Available at https://eur-lex.europa.eu/eli/reg/2024/2847/oj, 2024.

[4] Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation), Available at https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng, 2016.

[5] European Parliament, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations, Available at https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng, 2024. Accessed: 2025-12-17.
[6] Information technology — Security techniques — Information security management systems — Overview and vocabulary, Standard ISO/IEC 27000:2018, International Organization for Standardization, Geneva, CH, 2018. URL: https://www.iso.org/standard/73906.html.
[7] Information technology - Security techniques - Information security risk management, Standard ISO/IEC 27005:2018, International Organization for Standardization, Geneva, CH, 2018. URL: https://www.iso.org/standard/75281.html.
[8] Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model, Standard ISO/IEC 15408-1:2022, International Organization for Standardizqation, Geneva, Switzerland, 2022. URL: https://www.iso.org/standard/72891.html.
[9] E. Commission, The EU Cybersecurity Act, Available at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act, 2019. Accessed: 2025-12-17.
[10] A. Mantelero, The fundamental rights impact assessment (fria) in the ai act: Roots, legal obligations and key elements for a model template, Computer Law & Security Review 54 (2024) 106020.
[11] S. Bertaina, I. Biganzoli, R. Desiante, D. Fontanella, N. Inverardi, I. G. Penco, A. C. Cosentini, Fundamental rights and artificial intelligence impact assessment: A new quantitative methodology in the upcoming era of ai act, Computer Law & Security Review 56 (2025) 106101.
[12] D. Casaburo, I. Marsh, Ensuring fundamental rights compliance and trustworthiness of law enforcement ai systems: the aligner fundamental rights impact assessment, AI and Ethics 4 (2024) 1569–1582.
[13] P. Sirena, et al., Tre tesi sulla distinzione tra danno-evento e danno-conseguenza, BANCA BORSA TITOLI DI CREDITO (2023) 1752–1757.
[14] C. M. Bianca, Diritto civile, V, La responsabilità, 2a ed, 2012.
[15] Z. Syed, A. Padia, T. Finin, L. Mathews, A. Joshi, Uco: A unified cybersecurity ontology, 2016.
[16] C. Blanco, J. Lasheras, E. Fernández-Medina, R. Valencia-García, A. Toval, Basis for an integrated security ontology according to a systematic review of existing proposals, Computer Standards & Interfaces 33 (2011) 372–388.
[17] C. Blanco, J. Lasheras, R. Valencia-García, E. Fernández-Medina, A. Toval, M. Piattini, A systematic review and comparison of security ontologies, in: 2008 Third International Conference on Availability, Reliability and Security, 2008, pp. 813–820. doi:10.1109/ARES.2008.33.
[18] M. Adach, K. Hänninen, K. Lundqvist, Security ontologies: A systematic literature review, in: Enterprise Design, Operations, and Computing: 26th International Conference, EDOC 2022, Bozen-Bolzano, Italy, October 3–7, 2022, Proceedings, Springer, 2022, pp. 36–53.
[19] A. Souag, C. Salinesi, I. Comyn-Wattiau, Ontologies for security requirements: A literature survey and classification, in: Advanced Information Systems Engineering Workshops: CAiSE 2012 International Workshops, Gdańsk, Poland, June 25-26, 2012. Proceedings 24, Springer, 2012, pp. 61–69.
[20] S. Barnum, Standardizing cyber threat intelligence information with the structured threat information expression (stix™) (2014) 22.
[21] K. A. Akbar, F. I. Rahman, A. Singhal, L. Khan, B. Thuraisingham, The design and application of a unified ontology for cyber security, in: International Conference on Information Systems Security, Springer, 2023, pp. 23–41.
[22] B. A. Mozzaquatro, R. Jardim-Goncalves, C. Agostinho, Towards a reference ontology for security in the internet of things, in: 2015 IEEE International Workshop on Measurements Networking (M N), 2015, pp. 1–6. doi:10.1109/IWMN.2015.7322984.
[23] C. Blanco, D. G. Rosado, Á. J. Varela-Vaca, M. T. Gómez-López, E. Fernández-Medina, Onto-carmen: ontology-driven approach for cyber–physical system security requirements meta-modelling and reasoning, Internet of Things 24 (2023) 100989.
[24] R. Y. Venkata, R. Maheshwari, K. Kavi, Simon: Semantic inference model for security in cyber physical systems using ontologies, ICSEA 2019 61 (2019).

[25] Í. Oliveira, T. P. Sales, R. Baratella, M. Fumagalli, G. Guizzardi, An ontology of security from a risk treatment perspective, in: Conceptual Modeling: 41st International Conference, ER 2022, Hyderabad, India, October 17–20, 2022, Proceedings, Springer, 2022, pp. 365–379.
[26] C. Grigoriadis, A. M. Berzovitis, I. Stellios, P. Kotzanikolaou, A cybersecurity ontology to support risk information gathering in cyber-physical systems, in: Computer Security. ESORICS 2021 International Workshops: CyberICPS, SECPRE, ADIoT, SPOSE, CPS4CIP, and CDT&SECOMANE, Darmstadt, Germany, October 4–8, 2021, Revised Selected Papers, Springer, 2022, pp. 23–39.
[27] S. Ramanauskaitė, D. Olifer, N. Goranin, A. Čenys, Security ontology for adaptive mapping of security standards (2013).
[28] S. Fenz, A. Ekelhart, Formalizing information security knowledge, in: Proceedings of the 4th international Symposium on information, Computer, and Communications Security, 2009, pp. 183–194.
[29] A. Herzog, N. Shahmehri, C. Duma, An ontology of information security, International Journal of Information Security and Privacy (IJISP) 1 (2007) 1–23.
[30] mitre, defend mitre faq, Available at https://d3fend.mitre.org/faq/, ???? [Online; Accessed 2025, 7 march].
[31] R. Riesco, V. A. Villagrá, Leveraging cyber threat intelligence for a dynamic risk framework: Automation by using a semantic reasoner and a new combination of standards (stix™, swrl and owl), International Journal of Information Security 18 (2019) 715–739.
[32] C. Sánchez-Zas, V. A. Villagrá, M. Vega-Barbas, X. Larriva-Novo, J. I. Moreno, J. Berrocal, Ontology-based approach to real-time risk management and cyber-situational awareness, Future Generation Computer Systems 141 (2023) 462–472.
[33] O. T. Arogundade, A. Abayomi-Alli, S. Misra, An ontology-based security risk management model for information systems, Arabian Journal for Science and Engineering 45 (2020) 6183–6198.
[34] M. Khaleghi, M. R. Aref, M. Rasti, Context-aware ontology-based security measurement model, Journal of Information Security and Applications 67 (2022) 103199.
[35] T. Rintamaki, H. J. Pandit, Developing an ontology for ai act fundamental rights impact assessments, arXiv preprint arXiv:2501.10391 (2024).
[36] J. Hernandez, D. Golpayegani, D. Lewis, An open knowledge graph-based approach for mapping concepts and requirements between the eu ai act and international standards, AI and Ethics (2025) 1–12.
[37] D. Golpayegani, H. J. Pandit, D. Lewis, Airo: An ontology for representing ai risks based on the proposed eu ai act and iso risk management standards, in: Towards a knowledge-aware AI, IOS Press, 2022, pp. 51–65.
[38] D. Golpayegani, H. J. Pandit, D. Lewis, To be high-risk, or not to be—semantic specifications and implications of the ai act's high-risk ai applications and harmonised standards, in: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency, 2023, pp. 905–915.