
POLITECNICO DI TORINO

DEPARTMENT OF CONTROL AND COMPUTER ENGINEERING (DAUIN)

Master Degree in Computer Engineering

Master Degree Thesis

# Considering Security Measures Mitigations in Automatic Cyber Risk Assessment

Author: Nicoló Gallo

Advisor: Alessandro Savino
Co-Advisor(s): Nicoló Maunero

April, 2025

# Abstract

Over the past few decades, we have witnessed how the world around us has become increasingly digitalized. Technology deeply pervades our lives, causing an ever greater dependence on it. However, the evolution of cybersecurity has not been as fast, creating a gap that can be exploited by malicious actors and, therefore, increasing the possibility of attacks occurring and the severity of their consequences.

In this context, risk assessment has become increasingly important over time and attempts to automate it are becoming more and more common. However, these solutions often overlook how the implemented security measures influence the outcome of the process, focusing mainly on identifying vulnerabilities or threats.

This Thesis aims to make risk assessment operations simpler and faster for a cybersecurity expert by automating them, thus eliminating all those manual activities that did not allow the workflow to be more dynamic and fast to adapt to change. For this purpose, Pyra, an existing tool used to conduct the risk assessment of a network infrastructure, was extended by adding the information needed to model the implemented security mechanisms.

The proposed solution takes as input the ontology model of the target ICT infrastructure that is to be analyzed, extends with the necessary information on vulnerabilities and risks related to the assets. As output a report is produced that, while evaluating identified risk values, takes into consideration implemented cybersecurity mechanisms and how these may mitigate the risk. This approach is fundamental in presenting affective results for risk management prioritization by the organization.

The proposed solution, in particular, follows two different workflows to populate the ontology with the risks associated with each resource: on the one hand threat modeling is automated resorting to SWRL rules and ontology reasoners, and on the other hand known vulnerabilities and weaknesses information is identified and associated to the corresponding threats. This double approach allows us to have a more detailed view of the risks; first, risks are associated with identified vulnerabilities, while SWRL rules for threat modeling aim at filling those gaps that may happen by considering only vulnerabilities and reducing false negatives. It then uses the information on the security mechanisms connected to the various infrastructure assets to obtain, with a linear combination of the various information, a score that considers not only the probability and impact of the risk, but also how much that specific countermeasure mitigates the score.

The advantages of this approach are, first, supporting through automation activities of cybersecurity experts as well as reducing possible personal bias during the analysis; while at the same time providing a solution easily adaptable to various context and needs. In fact, given the necessary inputs, the analysis of information and inference of results are automatically calculated, so the solution is suitable to being adapted as needed.

Pyra is certainly a first step on the road to the automation of risk assessment, following which other studies and expansions will be necessary to be considered effective, but at the same time it lays the first foundations for exploring an approach that in the literature can be considered truly innovative.

# Acknowledgements

I would like to express my gratitude to my advisor, Professor Alessandro Savino. A special appreciation goes to my co-supervisor, Dr. Nicolò Maunero, for his invaluable advices and enduring guidance throughout the work. His knowledge, availability and patience have been crucial towards the thesis' progress. I'm also thankful to my family who constantly keep on supporting me and because of whom I could pass even hardest times peacefully. Lastly, I would like to thank all my friends and everyone who contributed, directly or indirectly, to the success of this goal.

# Contents

# List of Tables

# List of Figures

# Chapter 1

# Introduction

In a world where digital is now an integral part of our daily lives, influencing more or less directly every aspect of our habits, it is of fundamental importance to ensure its correct use. On the one hand, the advantages offered have certainly been revolutionary from many points of view, for example, the knowledge and the access to information has been democratized thanks to the advent of internet, several daily operations have been simplified thanks to automation, smart working but also social interaction have been made easily improving productivity and emotional well-being. On the other hand, the problems that can arise from the improper use of these systems risk canceling out the benefits: data violation may results in identity theft and privacy problems, cyber attacks may cause data loss or physical damage, the wide availability of internet can cause also misinformation and many more.

In fact, as statistics show, the possibility of exploiting these weaknesses to their advantage is of increasing interest to agencies, foreign governments and criminals.

The 2023 Cybersecurity Ventures Cybercrime Report predicts a rapid increase in damage costs associated with cybercrime. By 2025, cybercrime is projected to cost $10.5 trillion in damages – a substantial leap from the $3 trillion recorded in 2015. These damages represent the cost of data breaches, stolen funds, intellectual property theft, operational disruption, and post-attack recovery [21].

These data demonstrate how in recent years the trend has been the increase in attacks and their complexity, causing ever greater economic and social impacts, it therefore appears clear how important it is to invest in cybersecurity by adopting a proactive approach that allows for the advance assessment of any damage before it occurs in order to minimize the company's impact and costs. In this context, all those processes aimed at managing the organization's cybersecurity posture and mitigating the risks caused by vulnerabilities that affect its infrastructures take on an increasingly important role. However, since the sector is still immature, there is a lack of standards and conventions that allow this work to be carried out effectively and for this reason, the aforementioned operations are often carried out manually, resulting in them being slow, cumbersome and ineffective if applied in a constantly evolving sector.

The standard mostly known nowadays are, for example, ISO 27005, NIST 800 - 30, octave and many more [45]. They all have in common that they are composed of a set of informally descriptive step, leaving the expert the possibility to adopt his own practical

approach to do the work, creating the possibility that the outcomes will depend from the expert himself.

For this reason, it is common opinion that these types of processes will gradually become more and more automated in order to be able to provide reliable and effective results in less time while keeping up with the needs of the sector.

In this area, numerous approaches have been tested: from the purely qualitative ones, which mainly include the first standards developed, which are often manual and strongly depend on the opinion of the expert, to the more quantitative ones, which are generally preferred by those working in cybersecurity (86%) [28] These allow greater automation, but the difficulty in modeling all the factors that influence the process has meant that they have tended to be less effective because they are less flexible to the various cases.

Among these practices, cybersecurity risk assessment is certainly important, which consists in, given a network infrastructure, identifying and evaluating the risks that could affect the resources of the network in question.

In this context, our tool certainly presents itself as a promising solution because, being autonomous and automated, it helps to reduce costs and times, making it especially useful for medium and small businesses, which are usually those with fewer resources available.

Furthermore, unlike the current state of the art generally speaking, it also takes security mechanisms into account. In fact, in traditional threat modeling and quantitative risk assessment models, security measures are often not considered for the subsequent calculation of the resulting risk and this causes a wrong prioritization of the implementation scheduling of mitigation. Our thesis attempts, from this point of view, to lay a first brick in the road to the implementation of this.

In the IT field, security measures can be understood with different facets, for example they can be both physical elements of the infrastructure, or implemented algorithms but also good practices that the user should follow. Our thesis, being more oriented to the security of the physical infrastructure and less directed towards user modeling, leaves out this last factor, focusing more on physical countermeasures.

Risk assessment in these contexts is anything but simple, since it depends on numerous factors and varies based on the specific situation. Furthermore, addressing it in an analytical and quantitative way would require modeling all the elements involved, a task that is already complex at the identification stage and even more challenging when considering possible mitigation strategies.

This thesis aims to improve the risk assessment process, taking into account the security mechanisms and developing a method that allows to identify useful metrics and parameters for this purpose, providing a clear and applicable representation.

To do this, the development of the thesis started from a risk assessment tool, PyRA [12], previously developed during another work. From this, the knowledge base was enriched by introducing D3FEND as an additional database in addition to those already present in order to provide a better description of the techniques to mitigate possible attacks related to the infrastructure. From these databases, the tool extracts the risks that affect the infrastructure through two different workflows, but introducing factors related to the mitigation present in the final risk calculation. To do this, the main ontology was enriched with various information from other ontologies, among the most important those on security measures, in order to take the latter into account and thus have a more precise vision of the actual security condition of the system.

This approach meant that most of the process was automated while still guaranteeing high flexibility of modification and interpretation to the security expert.

The remainder of the document is organized as follows. Chapter 2 gives an overview of the main concepts related to the Thesis; in Chapter 3, the most important works related to the development of the tool are addressed, while our contribution is presented in Chapter 4. In Chapter 5 are reported and discussed the experimental results and, finally, in Chapter 6 conclusions are provided and possible future developments are outlined.

# Chapter 2

# Background

This chapter will introduce and explain the most important technical aspects, that will be useful to the reader throughout this document, to better understand the proposed solutions and results obtained. In particular, the concept of cybersecurity risk assessment will be presented, which sub-processes it is composed of and how these combine with each other to obtain the required results. A comparison will then be made of the models, frameworks, etc. currently used by the industry and their advantages and disadvantages, considering in particular their effectiveness in real contexts. An overview of the most commonly used categorizations of security measures will be presented below. Moreover, the traditionally most used methods to calculate the risk score will also be analyzed, and their effectiveness and limitations will be discussed.

The aim of this chapter is to guarantee the reader the necessary knowledge of the theoretical aspects, tools and problems related to risk assessment in the field of cybersecurity, highlighting the main critical issues and limitations of current methods. Furthermore, the existing tool on which this work is based will be presented, with an overview of its functionalities and the reasons why an improved approach is needed.

## 2.1 Cybersecurity Risk Assessment

In the context of cybersecurity, risk assessment is "The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigation provided by security controls planned or in place." [37].

### 2.1.1 Phases of Cybersecurity Risk Assessment

This process typically consists of the following phases, depicted in Figure 2.1:


Figure 2.1. 7 steps of cyber risk assessment

1. **Asset Identification**: this phase involves the enumeration of assets (hardware, software, data, networks, users, services) and the relationships and dependencies between them, considering their importance for the business in order to be able to take into account, as a starting point, those that are critical for the core business of the organization and those that are accessories and can be ignored in the event of a lack of budget.

2. **Threat modeling**: in this phase the most relevant threats are analyzed, taking into account various factors such as asset priorities or the categories of threats that are most exploited. This analysis is generally done taking into account the knowledge that can be derived from databases commonly used in this sector such as CVE, CWE, CAPEC, ATT&CK and D3FEND. In order to have a more complete vision, you can also try to think about how these threats can be exploited in a real attack.

3. **Vulnerability Assessment**: in this phase the known vulnerabilities are catalogued for each asset. This can be done through different tools or manually; moreover, information obtained from the MITRE CVE and possibly from proprietary databases

is used as well. Subsequently, all this information is correlated with the threats identified in the previous step.

4. **Risk Analysis**: during this phase the risk score is evaluated with the chosen approach, at the discretion of the expert or the organization, taking into consideration all the results obtained from the previous steps, in particular the following risk factor are estimated:

   - impact, which represents the potential damage caused by an attack and considers the possible financial and reputational losses, but also the legal and operational consequences, including the possible knock-on effects on other assets.
   - likelihood, which represents the possibility that the given event occurs and depends on the technical complexity in developing an exploit for the vulnerability or the already availability of these and the actual frequency of use.

5. **Risk Evaluation**: this phase consists in assigning risk levels through, for example, risk matrices or other tools and the subsequent comparison with the organization's risk appetite, in order to be able to draw a plan with the actions to be taken to mitigate the identified risks.

6. **Risk Treatment**: this phase is devote to understand how to address the identified risks. To manage the risk there are different approaches that depends on the context and organizational goals. It is possible to identify four main solutions, which should be selected for each identified risk: REDUCE, ELIMINATE, TRANSFER, and ACCEPT. If possible and convenient, security controls (REDUCE) derived from the planning are implemented, such as firewalls, Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS), backups but also staff training and policies. Otherwise, it is also possible to implement an ELIMINATION of the asset causing the risk in the event that the disadvantages in the event of an attack were greater than its role in the organization, or even TRANSFER the risk, such as insuring the corresponding asset or the corresponding attacks and finally ACCEPT the risk provided if it is economically justified and there is no other solution.

7. **Risk Monitoring and Review**: This phase is continuous and involves the periodic updating and re-execution of the entire process considering new possible threats and vulnerabilities, but also penetration tests and audits.

### 2.1.2 Risk Assessment Resources

In order to carry out these seven phases, the Risk Assessment process includes the use of different support resources that provide conceptual structures, data collections and methodologies that help the expert in the process. In order we can list [45]:

- Threat modeling methodologies, there are different types and with different levels of detail, they provide a structured approach to identify and analyze threats related to a given system. To do this, they are composed of different steps more or less articulated depending on the methodology.

- Vulnerability catalog, they collect and group information on known vulnerabilities for specific assets by formatting the data related to them in order to make them easier to use, they can be both public, such as CVE and NVD, but also proprietary.
- Attack libraries, in this case (similarly to what is done for vulnerabilities) tactics, techniques and procedures (TTP) used by a potential attacker to compromise the system are listed, the most known are MITRE ATT&CK and CAPEC, but also other databases on public exploits.
- Cybersecurity Controls frameworks, they are somewhat antagonistic to the previous ones and therefore deal with mapping possible methods, best practices or mitigation systems for each TTP to strengthen the organization's cybersecurity posture, in this category we can find, for example, MITRE D3FEND and CIS controls.
- Compliance frameworks, which establish standard practices that the expert should follow to develop the entire process, among the most known are certainly the ISO 27000-seires, NIST 800 and GDPR but in reality there are many more because each government, industry and company develops its own.

Each of these resources is not used in isolation but are often interconnected with each other,for example, threat modeling methodologies can leverage vulnerability and attack catalogs to derive adequate countermeasures from cybersecurity controls frameworks, all while following the directives dictated by compliance frameworks.

### 2.1.3 Introduction to D3FEND

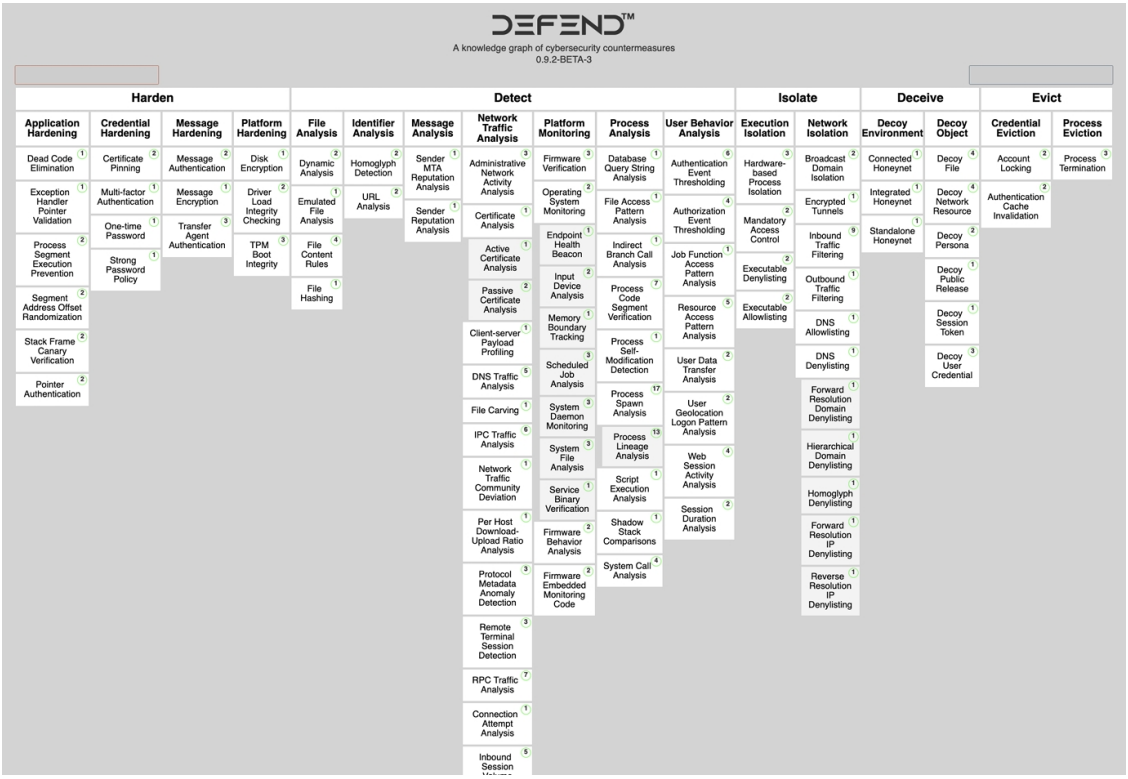


Figure 2.2. D3FEND matrix [29]

"D3FEND is a knowledge-base, but more specifically a knowledge graph, of cybersecurity countermeasure techniques. In the simplest sense, it is a catalog of defensive cybersecurity techniques and their relationships to offensive/adversary techniques. The primary goal of the initial D3FEND release is to help standardize the vocabulary used to describe defensive cybersecurity technology functionality." [35].

D3FEND was created as a counterpart to the widely recognized MITRE ATT&CK® Framework, which focuses on describing and categorizing adversarial tactics, techniques, and procedures (TTPs) in the cybersecurity domain [22]. The D3FEND matrix is presented in Figure 2.2

While the ATT&CK framework focuses on helping organizations understand and defend against cyber threats by detailing how adversaries operate, the D3FEND framework aims to provide a structured, systematic approach to implementing defensive cybersecurity measures. The D3FEND framework offers a common language and taxonomy for describing defensive techniques, enabling cybersecurity professionals to better communicate, collaborate, and develop more effective security strategies.

D3FEND framework covers various defensive techniques across multiple categories, including data protection, network defense, endpoint defense, identity and access management, and others. The framework is designed to be flexible and adaptable, allowing organizations to tailor their security strategies to their unique needs and threat landscape.

In addition to this, the D3FEND framework helps organizations make informed decisions about their cybersecurity strategies by providing clear, actionable guidance on defensive measures, but also promotes the adoption of best practices and proven security measures, helping organizations reduce their risk of cyberattacks and minimize the impact of successful breaches.

The D3FEND countermeasure guidance is arranged in a similar way to the ATT&CK hierarchy of TTPs [22].

The D3FEND hierarchy's highest classification is *Tactics*, each Tactic represents a defense objective related to a given stage of an attack. Within the Tactics are Techniques and Sub-Techniques describing the methods used to accomplish the Tactics' goals, including references to industry security standards and tools.

MITRE D3FEND also offers a hierarchical catalog of related information called *Digital Artifacts*, which is not included in MITRE ATT&CK. Digital Artifacts include digital objects and concepts split into four main categories: top-level artifacts, files, network traffic, and software. Some adversarial TTPs from ATT&CK can be mapped to D3FEND's Techniques, with Digital Artifacts serving as the reference for identifying related offensive measures and countermeasures.

## 2.2 Risk Assessment Framework and Standard

In this section, a categorization of risk assessment typologies will be presented, highlighting their main characteristics and differences. Furthermore, some frameworks used in the industry will be presented, linking them to the typologies described. Finally, the role of the expert and his relationship with the different methodologies will be discussed.

### 2.2.1 Types of Risk Assessment Methodologies

Generally when we talk about risk assessment methodologies these can belong to 5 macrotypes each with its advantages and disadvantages:

- qualitative approaches: they provide a not very structured and highly subjective approach and therefore dependent on the expert in charge since the risk score is usually chosen by him and not numerical, they are very versatile but at the same time very subject to the dangers of incorrect interpretation.

- quantitative: they tend to have a more scientific and methodological approach, they try to automate and discretize the process by assigning numerical risk scores, thus resulting objective and this makes the prioritization phase easier and more immediate, but they are more difficult to implement since there is not always enough data to quantify the associated risk and they cannot always be easily adapted depending on the use case.

- asset-based approaches: they start from the classification and prioritization of the infrastructure assets, they allow more rigor in the process but may mistakenly not consider risks associated with factors not dependent on listed assets.
- vulnerability-based approaches: starts from the evaluation of the possible vulnerabilities of a system, prioritizing them based on how much their exploit could cause damage to the organization.
- threat-based approaches: starts from the evaluation and classification of the possible categories of threats that the organization under analysis can be a victim of, considering the probability that this will happen.

However, these categories are not mutually exclusive, in fact they often intersect or even the solution adopted turns out to be a bit of a mix of several of them.

Some practical examples of these methodologies currently used in the industry today are ISO/IEC 27005, NIST SP 800-30 and FAIR (Factor Analysis of Information Risk). These offer structured frameworks for risk assessment, ISO/IEC 27005 and NIST SP 800-30 adopt a systematic approach, while remaining more qualitative since they leave the expert the freedom to adopt their own methods to develop the phases described below: risk identification, risk analysis (in which threats, vulnerabilities, probabilities and impacts are assessed) and risk assessment, comparing the values obtained with acceptable thresholds. On the contrary, FAIR brings in a quantitative perspective which assigns monetary value-based threats and therefore facilitates more detailed cost-benefit analyses.

Along with those general frameworks, there are additional more specific methodologies like DREAD, a qualitative model developed by Microsoft for classifying security risks, and OWASP Risk Rating Methodology, which provides a formula for calculating the risk of vulnerabilities. Other scoring tools, such as NIST CVSS and EPSS, can be considered other methodologies for calculating risk, helping to quantify the severity of the vulnerabilities under examination.

What all these methodologies have in common is that the role of the expert is a key element in the risk assessment process, in fact, this intervenes in different phases to understand the data and ensure that the analysis is contextualized with respect to the organization. In qualitative models, the expert's opinion is central to estimating the threats and potential consequences. In quantitative methods, however, the expert's judgment is required to select the correct parameters and verify the consistency of the metrics adopted. Among these types of models, the former are much more dependent on the opinion of the person conducting the assessment and therefore subjective and difficult to reproduce, however the role of the expert remains of primary importance to evaluate each context. To conclude, it was noted how in the end the most effective models combine automated tools with human contribution, ensuring a balanced assessment between objective data and operational context [45].

## 2.3 Introduction to PyRA

Our thesis extends and updates a previously developed tool, PyRA [12]. Here is a summary of its workflow and main architecture, depicted also in Figure 2.3:

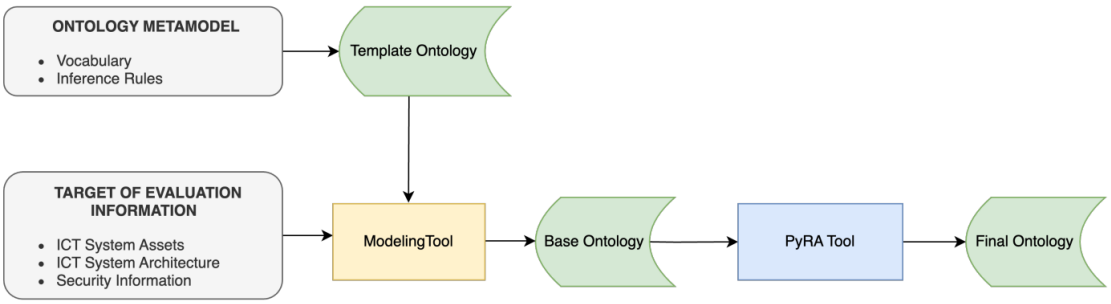


Figure 2.3. PyRA Workflow [12]

1. ICT Infrastructure Modeling: the first phase of the tool involves modeling the ICT system being evaluated through the ontology that will then act as a database for all subsequent operations. The modeled information includes the assets that make up the system and their typologies and the data flows between them, thus creating what is called the base ontology. In fact, the utility of the ontology lies in defining the entities whose properties and relationships between them will be inherited by the instances, thus defining the relationship between the various instances. In addition, it also uses a reasoner to verify that none of these rules are inconsistent. The ontology has been gradually developed and updated during various studies, for a more in-depth discussion, please refer to [14] and [12].

2. Threat modeling: PyRA then uses the reasoner and the SWRL rules defined in the ontology to infer the possible threats related to each asset of the system. This step allows to infer the threats without relying on the public knowledge given by the vulnerability databases but according to well-defined rules that, in doing so, can also take into account the relationships and data flows between the assets and how they interact with each other. For a more in-depth discussion of the rules see [15].

3. Analysis of the basic ontology: at this point, through a python script, the ontology is populated with information from the various MITRE and NIST knowledge bases to have a list of vulnerabilities for each asset. At this point, a populated ontology is produced in which both the threats that affect the system with their respective risk scores and the vulnerabilities associated with each asset are specified.

4. Report: From this ontology, various reports are produced showing the results found sorted by severity.

In summary, PyRA automates the collection of security data and uses the ontology reasoner to simplify the evaluation process and help in the mitigation process by providing an always updated view of the security posture of the infrastructure under examination.

# Chapter 3

# Related Work

In this chapter, the academic background related to cybersecurity risk assessment is explored, in particular the role of ontologies and how they can positively influence the process. The current approaches for modeling security measures and how their different implementations impact the final risk calculation will be explored. Along with this, the various methods used for the final calculation of the risk score will also be considered, how they relate to mitigation and their limitations when applied in real use cases. This chapter will present all these concepts by analyzing the current state of the art, highlighting strengths and limitations of the various approaches.

## 3.1 Ontologies overview

The first step in the development of the thesis was to find an effective way to somehow map the security mechanisms in the ontology, so that they could subsequently be used to model the possible countermeasures of the system. Conceptually for our thesis, countermeasures are prevention mechanisms that detect an incident/event, reduce or avoid a threat/the effects of an incident and/or protect an asset and its properties. It can be an action/approach that mitigates or prevents the risk and impacts of an attack or a measure that modifies the risk and mitigates the vulnerabilities defined by implementing physical or organizational measures [1].

To begin the research we started from existing reviews, trying to give priority to the most recent ones. Starting from these first results we expanded the set of possible sources using the bibliographies of the studies selected by the reviews. Finally, the search was concluded in a generic way through Google Scholar in order to be able to check that we had more or less taken into consideration all the papers, or at least the most relevant, for our purposes.

### 3.1.1 Review overview

Below is a brief description of the most useful reviews considered for the research:

- The work of Blanco et al. [8] presents a systematic review of existing ontologies. The main goal of the review is to identify the main features that an ontology should

have to correctly and extensively represent a security domain. In the end, the work concluded that, at the time of the review, there is still no solution that allows to map and effectively represent all the features as it would be necessary and therefore it is much more useful to have different specific ontologies for each domain.

- The work of Adach et al. [1] provides a comparison of the best general ontologies currently available. The study concluded, in line with the previous work, that each ontology has conceptual gaps and that therefore it is necessary to work to create a unified solution.
- The work of Souag et al. [46] 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.
- The work of Blanco et al. [9] updates the results from the first research noting how the improvements have still been too mild compared to the needs
- the work of Pastuszuk et al. [40] instead tries to make the risk assessment dynamic through the ontology using the integration of systems to populate the ontology with real-time data. Consistent with the other reviews, the study notes how the excessive integration of different cybersecurity domains drastically lowers the precision of these tools.

### 3.1.2 Ontologies overview

Table 3.1 summarizes the main result of the literature review regarding ontologies.

Table 3.1. Ontology Analysis Results

| **Source Ontology** | **Publicly Available** | **Generic or Specific** | **Development Level** | **Security Mechanism Modeling Quality** |
|---|---|---|---|---|
| UCO[48] | Yes | Generic | Decent | Poor |
| Unified Ontology[3] | No | Generic | Decent | Poor |
| Tsoumas and Gritzalis Ontology[49] | No | Generic | Good | Good |
| IoT Security Ontology[36] | Yes | Specific for iot | Good | Poor |
| OVM Ontology[53] | No | General | Medium | Medium |
| Core Ontology[44] | No | General | Bad | Bad |
| Pereira and Santos Ontology[41] | No | General | Low | Low |
| Ontology of Attacks[24] | No | General | Decent | Poor |
| NRL Ontology[33] | No | Web-Specific | Good | Not Suitable |
| MITRE ATT&CK Ontology[27] | No | General | OK | Not Suitable |
| Undercoffer, Joshi and Pinkston Ontology[51] | No | IDS-Specific | Medium | Not Suitable |
| Application Ontology[16] | No | App-Specific | OK | Not Suitable |
| Ontology for simulating threats[17] | No | General | Good | Not Suitable |
| Tsoumas, Dritsas and Gritzalis Ontology[50] | No | General | Zero | Zero |
| Ontology for Vulnerability[18] | No | General | Medium | Bad |
| Unified Knowledge Graph[10] | No | General | Medium | Medium |
| Standard-based Ontology[2] | No | Generic | OK | Poor |
| Herzog, Shahmehri and Duma Ontology[26] | Yes | Generic | Good | Top |
| Fenz and Ekelhart Ontology[23] | No | Generic | Good | Good |
| Herzog-Fenz Extension Ontology[43] | No | Generic | OK | Medium |
| D3FEND[29] | Yes | Generic | Top | Not Suitable |
| CIS CSC[13] | Yes | Generic | Medium | Not Suitable |

From these studies we have been able to note how a good number of the proposed ontologies was limited at modeling the general concepts of the ontology and therefore the main entities without going into detail for each class and the relationships between them.

Among those that had a considerable degree of development, we still need to filter out all those that did not have the ICT infrastructures as their field of application but were specific to a subsector such as IoT, web applications or IDS which therefore did not provide a useful modeling of security measures for our purposes. We also consider the level of development of the ontologies, extracted from the scientifical paper read. Another important factor in the evaluation of the ontologies is whether the latter were publicly available. Following all these observations, it can be noted how the solutions that could be taken into consideration were those of [26], [23] and [29].

### 3.1.3 D3FEND ontology

D3FEND, which was presented in 2.1.3, is certainly a promising research direction that, through the Digital Artifacts Ontology (DAO), tries to correlate attack scenarios with possible mitigation strategies. This approach is, in many respects, similar to the one we are developing in this work, but it presents some limitations that do not allow the application of D3FEND to this Thesis.

One of the main limitations of D3FEND is the level of abstraction at which it operates: it focuses on the conceptual modeling of defensive techniques and their relationships with offensive techniques, without providing an effective method to integrate this type of knowledge on specific network infrastructures or physical systems. This makes it less suitable for a risk analysis applied to an infrastructure, as it depends on a classification of attack scenarios that is not easily linked in an automated way to real infrastructures.

Furthermore, effectively representing certain security measures in a concrete way in D3FEND can be complex, since on the one hand it is very useful for having a classification of security measures, on the other hand it encounters difficulties in dealing with mitigation based on best practices and management measures.

Despite these limitations, D3FEND remains extremely useful within a cybersecurity knowledge base. Its value lies in the ability to provide, in a descriptive way, the possible mitigation that can be implemented in relation to the considered offensive techniques.

### 3.1.4 Fenz ontology

The work of Fenz et al. [23] highlights how the lack of managerial knowledge on cybersecurity is one of the main reasons why risk, in the corporate context, is managed ineffectively. For this reason, the aim of his work is to try to formalize and unify this knowledge through the use of ontologies to have a knowledge base that can facilitate risk management. Figure 3.1 summarizes the main element of the Fenz ontology.

The proposed ontology, based on the indications of the NIST, identifies the relationships between assets, vulnerabilities, threats and controls.

A threat represents a potential danger to the assets of the organization, which can materialize with the exploitation of a vulnerability. The latter can be physical, technical or administrative and are evaluated in terms of severity. To mitigate these vulnerabilities, controls are implemented that can be preventive, corrective, deterrent, recovery or detection. Furthermore, to ensure that the knowledge that represents the ontology is based on widely accepted and shared principles, the controls are derived from reference standards

such as the IT Grundschutz manual of Germany and the ISO/IEC 27001 standard. Furthermore, the ontology was developed using OWL-DL thus ensuring the possibility of use in automated systems.

The ontology has been divided into three main sub-ontologies: security, enterprise and localization. The first includes the fundamental concepts of threat, vulnerability, controls and evaluation systems and is the fundamental part of the model. The second sub-ontology, dedicated to the enterprise, allows to ontologically represent an organization and its environment, describing tangible and intangible assets, roles and relationships between actors. Finally, the sub-ontology that deals with localization allows to also take into account the data related to the position of the analyzed system to evaluate those threats whose probability is influenced by the geographical area in which they occur.

To evaluate the work done, a group of IT security experts performed an analysis to assess the effectiveness and completeness of the implemented work by asking questions in a formal and informal way to interrogate the ontology. Some issues identified through the analysis that need more accurate descriptions were: lack of concepts that represent the company's reputation, lack of a more elaborate evaluation method that could better quantify the effectiveness of security systems, and lack of information regarding the complexity in implementing the latter. These issues were addressed by introducing new concepts and improving the relationships between existing entities: new types of intangible assets such as company prestige and customer trust were introduced, and risk assessment methodologies were improved.

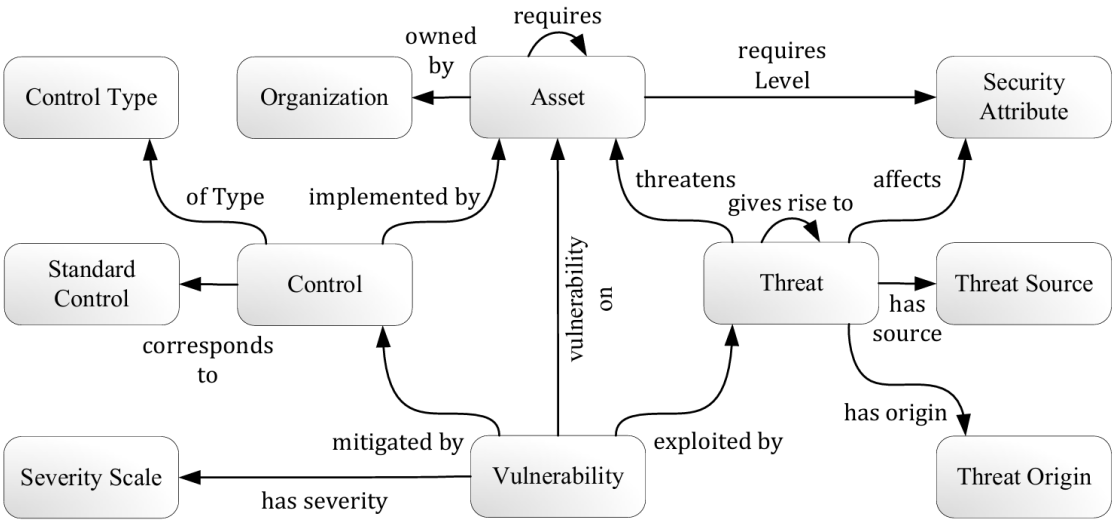


Figure 3.1. Fenz ontology [23]

It is interesting to note from the Figure 3.1 of the ontology of [23] how this aims to model the "security attributes", as we will see also does [26], linked to the concept of asset and threat. This idea will be useful later to develop our model for calculating residual risk.

In conclusion, the work presented is very promising for our purposes, however the corresponding ontology has not been made public and in addition to this in the paper [43] the two ontologies are compared and in relation to the available security standards. From the proposed comparison it emerges that both ontologies are still very far from completely mapping the concepts exposed in the standards and to solve the problem the proposed paper tries to formulate its own ontology. Even in this case the ontology is not available, however the author, during the study, states that the security measures modeled by [26] are described quite well and therefore decides to adopt those by making only small changes.[43]

### 3.1.5 Herzog ontology

The paper [26] proposes an ontology based on OWL to model in its entirety all aspects related to cybersecurity, starting from the representation of the main concepts that are: assets, threats, vulnerabilities and countermeasures, and the relationships between them. The work has been developed with the aim of providing a common vocabulary, a conceptual roadmap and an extensible dictionary for the cybersecurity sector. Figure 3.2 summarizes the main elements of the Herzog ontology.

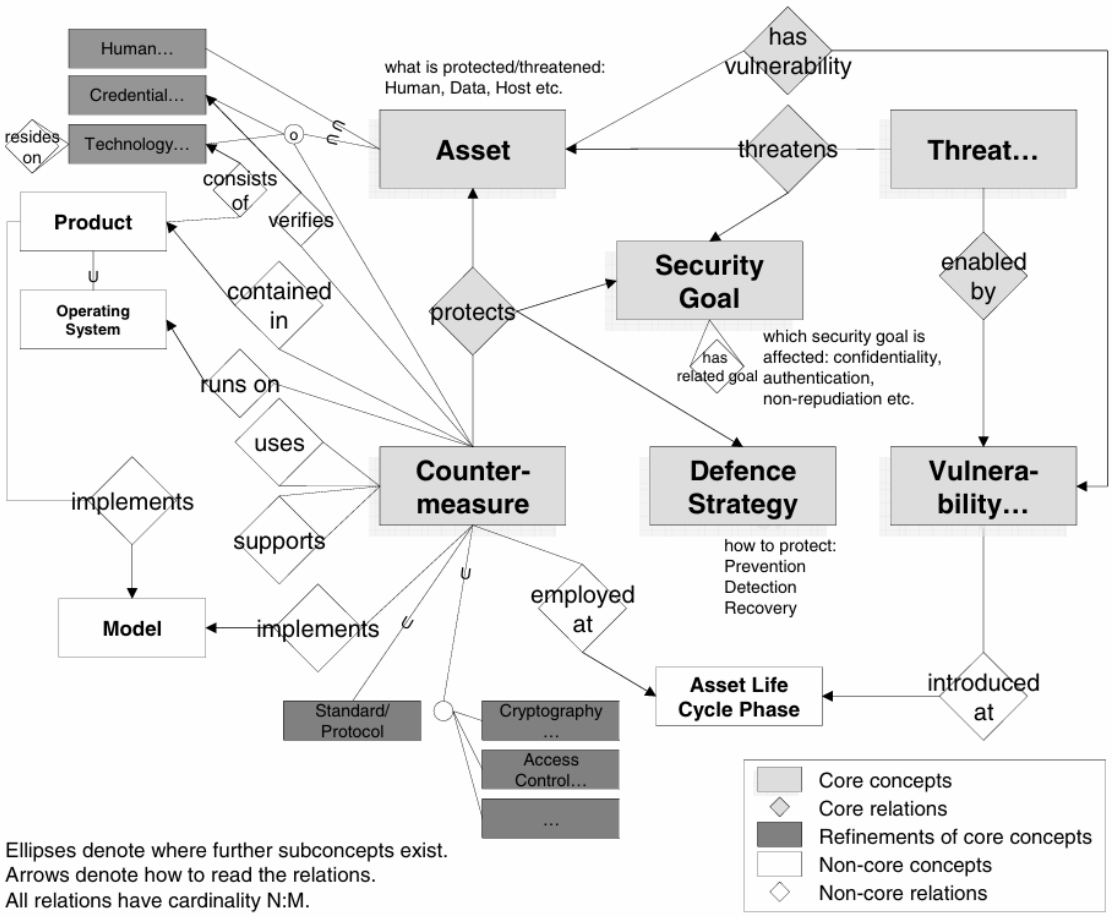


Figure 3.2. Herzog ontology [26]

The goal of Herzog's ontology is to first of all define a clear, structured and unambiguous reference framework since very often in this sector the lack of defined conventions leads to interpretative errors and consequently affects the quality of security decisions

The proposed ontology, similarly to [23], starts from the modeling of the 4 main entities: assets, which represent all those elements that have a value for the organization, threats, which are events or actors that can cause the compromise of the security of the assets, vulnerabilities, weaknesses that can cause the occurrence of a threat and countermeasures, designed with the aim of mitigating threats and consequently protecting the assets and the security properties connected to them.

The goal of the development was to create a general ontology that therefore represented the cybersecurity domain as extensively as possible but at the same time specific which models in detail each aspect considered.

To do this, starting from the four main concepts, they have been expanded and organized

into subcategories:

- assets can be physical, technological or human
- threats are divided into active and passive
- vulnerabilities which are the least extensive of all
- countermeasures which are classified according to their function and specify through their properties what they protect and what type of protection they offer

Figure 3.3 provide the complete view of countermeasures contained in the Herzog ontology.

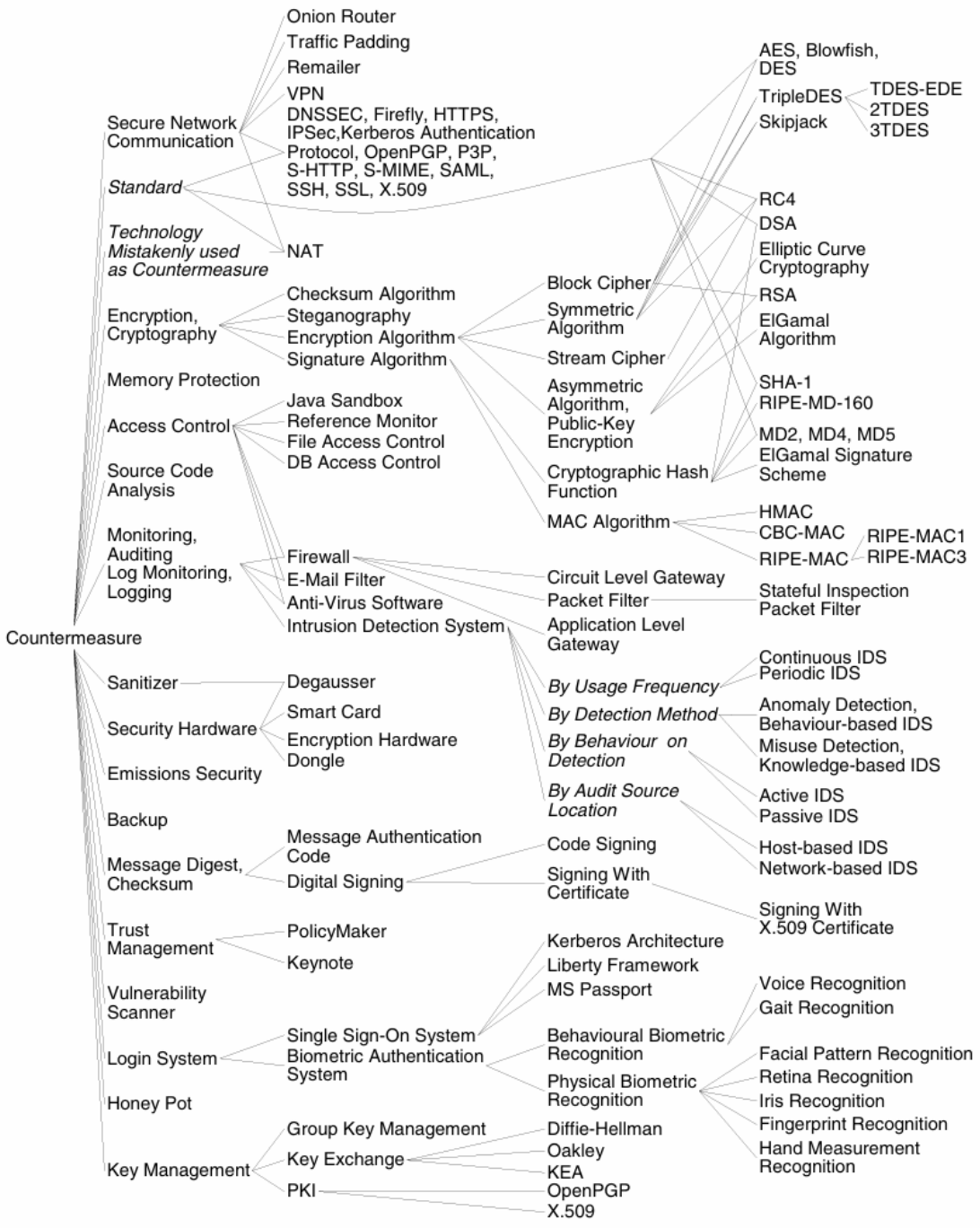


Figure 3.3. Herzog Countermeasures [26]

## 3.2 Risk Evaluation Methodologies

The definition of risk calculation methodologies is a task as fundamental as it is little developed in this field of research. The main approach involves the quantification of some values that will then be used to calculate the actual risk, among these values the most used are impact and likelihood. Both are obtained using historical and probabilistic data that, through the opinion of an expert, are mapped to certain values that in a more or less informal way correspond to what would be the damage produced if the threat were to come true and what would be the probability of this happening.

### 3.2.1 Tradional approach

The most commonly accepted method for calculating risk in the context of a risk assessment is based on the quantification of impact and likelihood.

Impact represents the consequences in terms of financial, operational, reputational and legal damages if a threat were to occur. Some examples of these types of damages can be:

- financial, representing the direct and indirect cost associated with an attack. For example, loss of revenue due to service interruptions, system recovery costs or possible customer compensation.
- operational, concerning the interruption of business processes and the consequent lack of service provision. In the case of a DDoS attack, for example, which makes a company website inaccessible, it can block online transactions for several hours or days, with negative consequences on the provision of the service. In these cases, the impact translates into a drop in productivity and delays in daily operations, with additional economic costs related to crisis management.
- reputational, occurs when an incident changes the perception that people had of the affected organization, resulting in loss of customers and consequently financial. Reputational damage may not be immediately noticeable but it has a long-term impact on the value of the brand and on possible relationships with other business partners.
- legal and compliance, this may include, for example, the costs resulting from sanctions due to the violation of data protection regulations (GDPR), or the costs of forensic investigations.

These different types of damage are usually estimated through the analysis of historical data relating to similar incidents, integrated with the experience of specialists in the sector. This analysis allows us to informally map the losses that an attack could cause, translating them into numerical values that feed the overall risk calculation. For example, in the case of a ransomware attack that historically led to losses of an average of 200,000 euros in operational and financial damage, but in some cases the damage that may have been caused by the change in reputation was much worse, the expert, taking this factor into account, can assign a higher value to the expected impact for that threat.

Likelihood, instead, indicates the probability that a certain attack will occur and this probability is defined through the combination of empirical data with the expert's opinion, the factors that contribute to the determination of this value are:

- historical frequency of attacks: thanks to the analysis of past incident logs, both internal such as system logs or reports but also external such as databases or public reports, it is possible to determine the number of times an attack has occurred in a certain period of time and therefore obtain a value that represents this frequency.
- factors regarding vulnerability: if the vulnerability associated with a threat has publicly available exploits, its exploitation does not require particular technical skills or the available attack surface is considerable, the probability is greater. To evaluate these factors, one can refer, for example, to the metrics reported in the CVSS.
- threat intelligence reports: reports from sources such as CERT, security vendors and research communities, provide up-to-date information on attack techniques, in fact their analysis reveals variations and emerging trends such as the increased use of a specific vulnerability or the use of new attack methodologies.
- system logs, through the analysis of logs produced by monitoring systems, which constantly record network traffic, it is possible to identify anomalous trends or traffic peaks that may be indicators of attack attempts.

The integration of these data with the interpretation of experts, through the use of qualitative scales (for example: low, moderate, high) or semi-quantitative, allows to determine in a more precise and updated way the probability that a threat will actually be exploited.

Once these two parameters have been obtained, the total risk is calculated as described in the the Figure 3.4, allowing to have an immediate vision of the risk associated with the different threats, although the method has some limitations in terms of subjectivity and dynamic updating capacity.

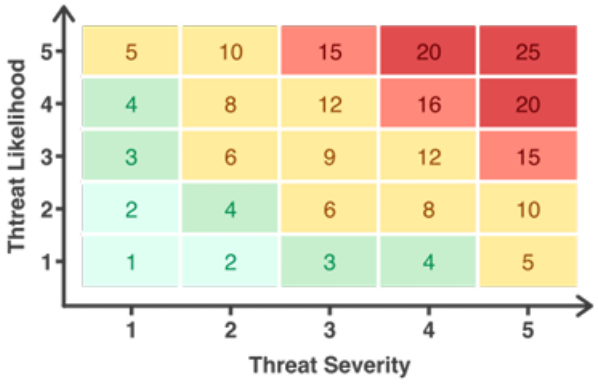


Figure 3.4. Risk matrix

### 3.2.2 Other methodologies

In the context of risk assessment in cybersecurity, numerous approaches have been explored. Research papers have proposed methods that integrate empirical data, network

measurements and other metrics along with expert assessments. These approaches can be divided into three main categories: quantitative, qualitative and semi-quantitative, which differ in how the risk is calculated and how much this operation depends on the expert's opinion.

### Quantitative methods

Quantitative methods typically address the problem using mathematical or statistical models and data derived from real-world event measurements to provide numerical estimates of risk. An example of this can be considered approaches based on Monte Carlo simulations that use these data to generate probability distributions, thus making it possible to numerically estimate the risk associated with certain threats. For example, studies such as [19] extend the concept of Cyber Value-at-Risk (CVaR) through Monte Carlo simulations: in this approach, the value of assets, the probability of threats and the effectiveness of security controls are integrated to estimate the distribution of losses and model the residual risk. Another quantitative technique is the one that involves the calculation of the Annualized Loss Expectancy (ALE), which, through the formula ALE = SLE * ARO, estimates the annual economic loss expected due to a threat. In the formula the terms SLE(single loss expectancy) and ARO(Annual Rate of Occurence) represent, respectively, the economic loss of a single incident and the expected frequency of the event in a year and both are derived from data of past events. Similarly, the FAIR model uses economic metrics according to the formula R=LEF×LM where the frequency of the loss event (LEF) depends on how many times a threat occurs and the probability that the threat event is successful while the magnitude of the loss (LM) is influenced by both direct damages and indirect damages to the organization. Alternatively, Bayesian networks are used to model the probabilities conditioned on the occurrence or non-occurrence of other events as in [52] where the FAIR model is extended with Bayesian graphs or also in [42] where the probability is updated in the presence of new compromises, therefore starting from the probability of the single event, considering the other compromises and calculating the final risk as the overall probability multiplied by the expected loss. These methods use objective data such as incident logs, industry reports and vulnerability databases, allowing estimates to be continuously updated based on new evidence.

### Qualitative methods

Qualitative methods rely primarily on expert judgment and descriptive risk categorization, without the use of precise numerical scores. In this approach, domain experts evaluate factors such as attacker capability, asset criticality, and operating conditions, assigning descriptive labels such as "low," "moderate," or "high". The DREAD model depicted in Figure 3.5 and Figure 3.6, for example, assigns scores based on parameters such as damage potential, reproducibility, and ease of exploit, from which it then derives impact and likelihood values. Another approach is proposed in [25], where matrices are used to correlate expert-judgment values related to assets, vulnerabilities, threats, and countermeasures, which can then be used to calculate the resulting risk by multiplying them. Additionally, studies such as [34] and [6] use structured questionnaires to gather the opinions of specialists within the organization, integrating subjective assessments into the decision-making

process. Such approaches are particularly useful when objective data is scarce or when it is necessary to capture the qualitative complexity of emerging threats.

| | High (3) | Medium (2) | Low (1) |
|---|---|---|---|
| **D** | The adversary is able to bypass security mechanisms; get administrator access; upload/modify the CPS content. | Leakage of confidential information of the CPSs (functions/source code); partial malfunction/disruption of the system. | Leakage of non-sensitive information; the attack is not possible to extend to other CPSs on-board. |
| **R** | The attack can be reproduced at anytime. | The adversary is able to reproduce the attack, but under specific risk conditions. | Although the attacker knows the CPS's vulnerabilities/faults, they are unable to launch the attack. |
| **E** | The attack can be performed by a novice adversary, in a short time. | A skilled adversary may launch the attack. | The attack requires an extremely skilled person and in-depth knowledge of the targeted CPS. |
| **A** | All CPSs are affected. | Some users/systems, with non-default configuration are affected. | The attack affects only the targeted CPS. |
| **D** | The CPS's vulnerabilities are well known, and the attacker is able to access the relevant information to exploit them. | The CPS's vulnerabilities/faults are not well known and the adversary needs to access the CPS. | The threat has been identified, and the vulnerabilities have been patched. |

Figure 3.5. DREAD criteria to evaluate risk level

$$Impact_t^s = \frac{Damage + Affectedsystems}{2},$$

$$Likelihood_t^s = \frac{Reproducibility + Exploitability + Discoverability)}{3},$$

$$Risk_t^s = \frac{(Impact_t^s + Likelihood_t^s)}{2}.$$

Figure 3.6. DREAD formulas to calculate risk for threat t and system s

### Semi-Quantitative methods

Semi-quantitative methods are a compromise between the deterministic approach of quantitative methods and the flexibility of qualitative ones. In this case, the expert assessments are converted into numerical values through the use of standardized scales, allowing more accurate comparisons between different risk scenarios. One of the most used approaches of this type is the CVSS score, which assigns a score based on parameters such as ease of exploitation and potential impact, combining qualitative assessments such as "easy" or "difficult" to exploit with numerical indicators. Other methods involve processing data from expert opinions to be able to automate them later, such as in [7] where opinions are represented by probability distributions that are convolved to obtain a shared opinion, or in [20] where CTF exercises with different scenarios and applied to different security experts are used to obtain experimental data on the effectiveness of countermeasures. Or other methods include the use of attack trees as in [31] where the difference between the graphs before and after the insertion of mitigation is made to obtain the residual risk. Many studies also take into account different metrics derived from the network structure and configuration such as: [39], [30] use these measurements to evaluate the effectiveness of countermeasures, while [47] and [5] improve the risk estimation by integrating the static risk with the current conditions and the proximity to untrusted networks, or again [4] and [32] that define the risk as a function of the asset value, the service exposure, the exploitability and the impact of vulnerabilities or considering the CVSS of the associated vulnerabilities and other metrics based on Confidentiality, Integrity and Availability. Other hybrid approaches integrate historical data – such as the number of accidents recorded in a sector – with subjective assessments by experts, thus providing an overall index that, although not completely numerical, allows for a more detailed comparative analysis than a purely qualitative one. These methods are generally considered semi-quantitative because they always start from the subjective assessment of the single risk, which is then improved by the available metrics.

## 3.3 Discussions

The approaches explored, as can be seen from the research, are multiple, ranging from purely qualitative ones to rigorously quantitative ones up to a combination of both. However, none of these methods is considered by the scientific community as the definitive method or at least the most promising one that solves a good part of their limitations. The shared opinion is that quantitative methods are the way to go because they allow a greater degree of automation, but it is also true that the expert's opinion is always one of the main factors that contribute to the calculation of risk to allow the model to be versatile and adaptable to every situation.

In this context, our study proposes a semi-quantitative approach that can be used in a passive environment such as the representation of a network infrastructure, from which it is not possible to obtain all those parameters useful for creating probabilistic estimates that represent the possibility of an event occurring.

In any case, it is commonly accepted among professionals in the sector that this would be an area that would need a substantial step forward, the available solutions are always late by definition and the importance that a correct prioritization of threats can make is

fundamental for the development of the sector. This entire subject of measuring residual risk is a bit of an elephant in the room for the cybersecurity industry [28].

# Chapter 4

# Contribution

In this Chapter, the main activities carried out during the research and the modifications made to the existing tool to include security measures in the risk calculation process will be presented. We will start with a description of the workflow of the tool modified with respect to the previous thesis, continuing then by describing the first accessory modifications made to the tool, including the integration of D3FEND and the description of the script for the categorization of CAPEC. Subsequently, the modifications made to the ontology will be explained, both as security measures and as the introduction of a new class representing the risk. Finally, we will present the function implemented for the calculation of the residual risk considering all the other modifications made.

## 4.1 Modified Architecture

The process, following the workflow reported in Figure 2.3 , begins with the development of the Template Ontology, in which all the information needed to subsequently represent the analyzed network infrastructure are defined. In particular, during this phase the main classes, their properties and the relationships between them are established. During our work we have extended and improved the modeling of the security measures described in the framework.

Subsequently, this ontology is imported into the Modeling Tool, in our case Protégé, and enriched with information on the ICT system to be analyzed (assets, typologies, data flows, security mechanisms), thus generating the Base Ontology.

The Pyra tool analyzes the base ontology, collects and organizes data taken from public sources to identify vulnerabilities and attack techniques, infers threats and calculates a risk score taking into account the mitigations provided by the security measures. At this stage, compared to the framework developed in [12], the tool enriches the ontology with information obtained from D3FEND to represent the mitigations associated with attacks in order to provide a more appreciable vision of the security posture of the infrastructure.

In this Thesis, also, the risk class in the ontology has been formalized, which will then be populated by Pyra, and the function for calculating the mitigated risk has been implemented.

The threat inference phase is divided into two distinct workflows: on the one hand

through pyra and the information obtained from BRON, a database that groups and relates all the information coming from public sources (see [12]), and on the other through the threat modeling rules developed in [15]. As for this last workflow, a script has also been written that allows completing the categorization of the missing threats. It was decided to select this approach to have a more complete vision, which on the one hand could be excessive, including some cases that may not represent a concrete risk (thus introducing some false positives). On the other hand, due to the limitations in the relationships between the databases, it may not obtain all the actual risks by underestimating them.

The description of all these phases and the changes made will be explored in the following sections.

## 4.2 D3FEND Integration

The tool presented in the work of [12] uses many publicly available databases, including CVE, CWE, CAPEC, ATT&CK, NVD, CPE, CVSS, to derive a complete knowledge-base on which to base computations and obtain the desired output. For a more in depth discussion refer to [12]. In addition to the above-mentioned databases, MITRE D3FEND (Detection, Denial, and Disruption Framework Empowering Network Defense) was added during this Thesis to expand the tool's knowledge-base.

In this section we will talk about the vulnerability sub-ontology, what it is composed of, what it is used for and how during our work it has been integrated with D3FEND's knowledge.

The Vulnerability sub-ontology is designed to model vulnerabilities that impact ICT infrastructure assets. The class is composed of several properties, such as:

- CVSS, represents the severity score of the vulnerability with a value ranging from 0 to 10
- Verified, if verified by the security team
- Mitigated, if mitigated

Each vulnerability is associated with an asset through the hasVulnerability relationship and is related to other classes such as:

- CVE: Identifies a public vulnerability, with data such as description, BaseScore, BaseSeverity and VulnStatus.
- CWE: Represents weaknesses in software/hardware that can cause vulnerabilities. It includes Name, Description and CommonConsequence (with details on security impacts). It is linked to CWE MITIGATION to suggest mitigations.
- CAPECs: series of CAPEC entries derived from the corresponding weaknesses, describing the risks associated with the vulnerability.
- ATT&CK: Describes attack tactics and techniques related to vulnerabilities.
- D3FEND: provides a description of the possible countermeasures that can be used to mitigate ATT&CK techniques.

The purpose of this sub-ontology is to provide a detailed view of the vulnerabilities related to the infrastructure and how these can be exploited in an attack and mitigated, supporting organizations in conducting a vulnerability assessment. For a more accurate description of the sub-ontology [12].

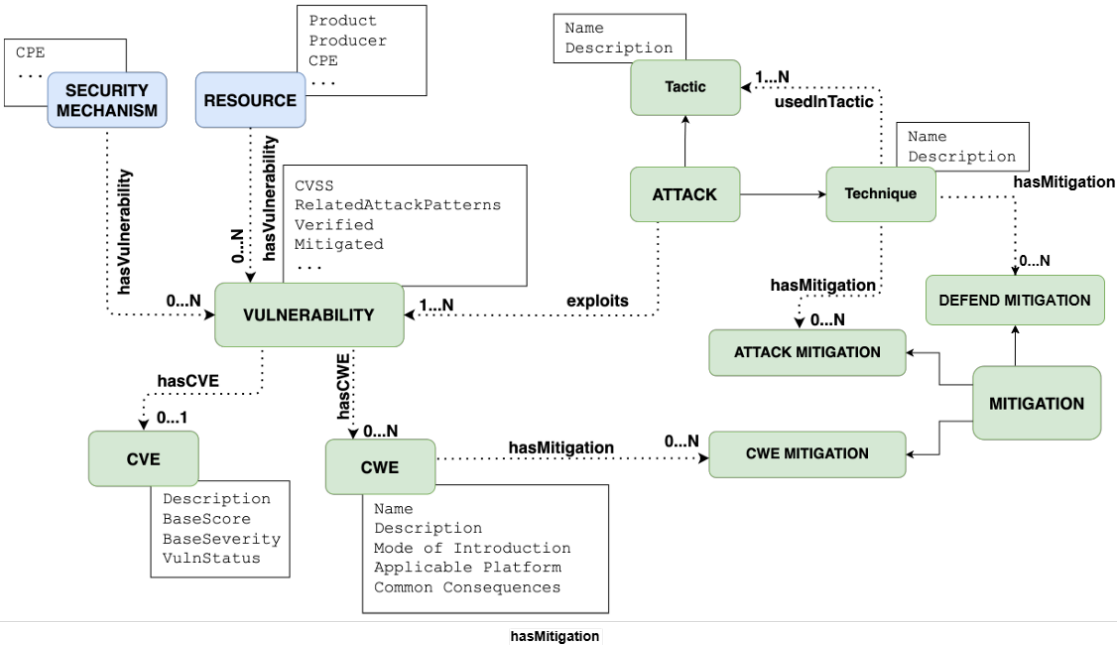


Figure 4.1. Vulnerability sub-ontology with D3FEND

At the current state of development, the knowledge derived from D3FEND is intended to provide for the selected vulnerability and the corresponding attacks a description of what could be the possible countermeasures to mitigate the considered attack. For future developments, it would be interesting and useful to find a way to connect the knowledge derived from D3FEND to the security mechanisms of [26], in this way a greater modeling power could be exploited. Currently, however, the measures used by us were too conceptually distant from those proposed in D3FEND and therefore the fusion between these two approaches would have been a manual and not "complete" operation because it would have been, in the current state of the tool, not very exploitable. This solution would instead be very effective if the focus of the risk assessment was moved from CAPEC to ATT&CK, in this case the mitigation of D3FEND would certainly be more representative and effective, but a way should be found to link them to the representation of the infrastructure.

## 4.3 Risk sub-ontology

In this section, similarly to what [12] did for the vulnerability sub-ontology, an overview of the risk class will be presented, its relationships with the other classes it is composed of and their role in defining and representing the information related to the class, as well as an evaluation of the design choices made for its implementation.

### 4.3.1 Motivation

In our context, the "Risk" class was introduced to represent the threats to which a given asset can be exposed in our infrastructure. The class is useful, in the risk analysis phase, to collect and aggregate all the information that will be necessary to calculate the risk score for each asset, taking into account the existing countermeasures.

The instances of the Risk class are generated within the tool starting from the instances of the Vulnerability class. This process occurs for each asset of the infrastructure, checking whether there is already an instance of the Risk class associated with the same combination of CAPEC and assets representing the vulnerability instance. In case a corresponding instance is already present, the vulnerability taken into consideration would simply be linked to the Risk instance found, thus avoiding having redundant instances and the cause of possible inconsistencies. Otherwise, a new instance is created to which assets, CAPEC and the vulnerability considered are linked, allowing the risk to be represented in a structured and coherent way.

### 4.3.2 Relationships with other classes

The Risk class is directly linked to other entities of the ontology to ensure availability and speed of access to information useful for assessing the risk of the infrastructure resources, whether this is done through the ontology itself or through the generation of the report.

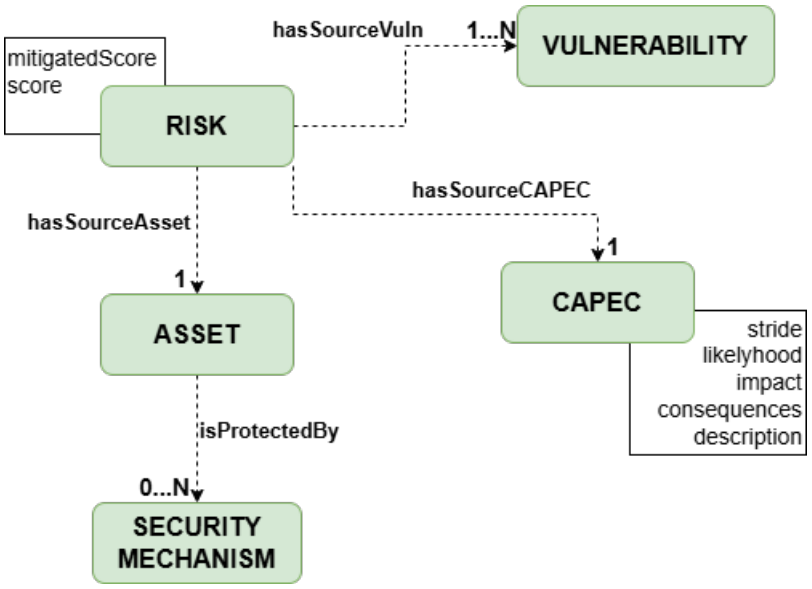


Figure 4.2. Risk sub-ontology

- Relationship with the Asset class and Security Mechanism: Each instance of the Risk class is linked to exactly one resource through the "hasSourceAsset" property. This connection allows to identify which components of the infrastructure are exposed to threats and indirectly makes it possible for the tool to retrieve all the security measures used to protect the asset in question. This relationship links the asset instance to the security mechanism instance through the "isProtectedBy" property and is necessary for the tool to retrieve the information that will then be useful to calculate the mitigated risk score.

- Relationship with the CAPEC class: The risks derive from specific threats and are modeled through the CAPEC class, which is connected to the risk instance through the "hasSourceCAPEC" relationship. In turn, this class, to exhaustively represent the risk, reports information such as: the STRIDE category, useful for categorizing the various CAPEC entries, severity and likelihood that respectively represent the impact that the threat could have and the probability that it will be exploited, and the consequences that instead indicate which are the security properties affected by the threat. In addition to this, descriptions are also provided in the form of comments that have the purpose of explaining how the threat works and how it could be exploited.

- Relationship with the vulnerability class: During the creation of all the instances of "Risk" the vulnerability connected is also tracked through the "hasSourceVuln" relationship, this allows, in addition to an improved navigability of the ontology, the possibility of tracing precisely which vulnerability caused the described risk. This operation is done in PyRA when the risk instance is created, it is checked that there is not already an instance with the same assets and CAPEC and if not it is created

and linked to the vulnerability, otherwise the vulnerability in question is simply linked to the instance found.

In addition to these linked classes, two properties have also been reported that represent the original risk score given by the threat and the same score modified according to the implemented security measures. This design choice allows not only to have the new risk more consistent with the infrastructure but also gives the possibility of comparing it with the original one, in order to evaluate the effectiveness of the countermeasures.

### 4.3.3 Evaluations on the implementation

To evaluate the inclusion of the Risk class in the ontology we took into consideration different solutions before deciding which one to apply in order to balance expressiveness, ease of use and computational complexity. On the one hand, a detailed modeling allows a more direct and simple use, while on the other hand we did not want to adopt a choice that would impact too much on the size of the ontology and the consequent computational cost.

The goal was to have an entity or in any case a part of these classes used to save the mitigated score, it could also be calculated directly during the report generation phase, and this would have avoided having to create the instances of the risk class and thus weighing down the ontology, however we wanted to provide, in addition to the report, the possibility of navigating and querying the ontology itself.

To do this, there were two possible paths: either the mitigated score linked to each CAPEC obtained could be integrated into the instances of the vulnerability class, or an instance of the risk class should have been created where the mitigated score could be saved together with the pairs (asset, CAPEC). The first solution would have allowed the desired information to be represented by adding only a string property to the vulnerability class, however, doing so would have made it more difficult and above all confusing to recover the information once necessary because they were all conceptually mixed in the same class. For this reason, in the end, we opted, similarly to what was done for the vulnerability class, to create this new class that would represent unequivocally and more clearly the combinations of (asset, CAPEC, mitigated score), at the cost of accepting a greater number of instances in the ontology that in the worst case would have increased by:

$$\#(risk\_class) = \#(CAPEC) * \#(asset) \tag{4.1}$$

Remembering that the cardinality of CAPEC is 559, it is potentially problematic in the case of complex infrastructures.

In conclusion, the risk sub-ontology provides a solid and ordered knowledge base from which to build the ICT infrastructure security report. Although its implementation involves a certain increase in the complexity of the ontology, the ability to evaluate and manage risk in a systematic way fully justifies this design choice.

## 4.4 Script for CAPEC Cathegorization

As previously described, the risk assessment is performed following two different workflows, to perform the one with the threat modeling rules, the categories of the various threats

populated with all of these are necessary. These categories were already present and were divided according to the "domains of attack" view of CAPEC, taking into account the categories with some meta-type subcategories. During the thesis we started from the situation in which the categories were populated by hand with some CAPEC and we extended, with the help of a developed script and with an Excel in input representing the hierarchies, the categorization to all the CAPEC entries of interest. At the moment, those regarding physical security and social engineering have been left aside because they are not useful for the modeling of our tool.

## 4.5 Ontology modification

Below we will present the changes made to the ontology to represent the security measures class in more detail, how they relate to and integrate within the ontology, and a helper class used to define more complex rules than are possible with OWL.

### 4.5.1 Starting Point

The adaptation of the representation of security mechanisms within the ontology was motivated by the need for a more concrete modeling that adheres to the real implementations of countermeasures that can be used in an ICT infrastructure. Initially, the proposed model provided a more abstract representation of security mechanisms, with generic classes that described categories of mitigation, including:

- AuthenticationMechanism
  - LoginSystem
- Crypthographic concept
  - KeyManagement
  - Encryption
  - MessageDigest
- SecurityManagementSystem

Although this approach was only a draft of a future implementation, it was limiting when it came to modeling security measures considering their relationships with infrastructure assets, so it was decided to opt for an alternative closer to a model that could physically and more concretely represent the possible countermeasures that can be used in an ICT infrastructure.

### 4.5.2 Herzog Security Mechanism

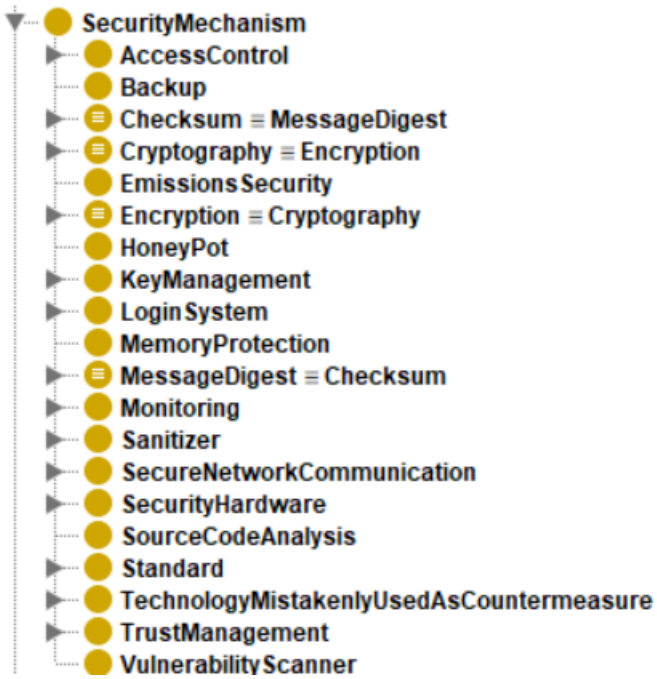


Figure 4.3. Security mechanism in Protégé

By adopting [26]'s solution, security measures are described by a more detailed structure, which directly represents the different available countermeasures, so that each class of the ontology can more faithfully reflect the solutions that can be adopted in practical scenarios. These classes are organized in a hierarchy that defines even the most abstract concepts at the highest levels, while as you go down into the child classes the representation becomes increasingly detailed and closer to the physical world (Figure 4.3 depict the first level view of these classes in Protégé).

An example of this is the Access control class that represents an abstract concept regarding access control in general, therefore to Hosts in the network but also to files or databases. Going down the hierarchy the abstract concept becomes more and more concrete with the subclasses for example FileAccessControl, Firewall and DBAaccessControl, and going down again for example into the children of Firewall you can find different types of practical firewall instances. In this way, in addition to remaining the possibility of representing generic concepts, it is also possible to specify the type of traffic that can filter, the supported protocols and the filtering strategies implemented. The same goes for other mechanisms, such as Login Systems, now modeled with specific attributes for supported authentication methods (e.g. password-based, multifactor, biometric).

This feature is made possible thanks to the different properties that a security mechanism can have, among the most important:

- protects, this property allows to unequivocally define the combinations of asset type, defense strategy type and security goal, modeled through the use of the NaryRelation class which is discussed in more depth in the Chapter 4.5.3. For example: The countermeasure ‘backup’ protects the integrity and availability (security goals) of the asset ‘data’ through recovery (defense strategy). As we will see in the Section 4.6 these rules will be fundamental for the development of this thesis because they will be the rules used to derive the mitigated risk score of the various threats.
- use, specifies whether a countermeasure is composed or can use several other countermeasures, for example ’SSL’ uses ’symmetric encryption’ and ’public-key encryption’.
- verifiesCredential, used when a countermeasure can verify credentials.
- supportedBy, when a countermeasure is supported by another, ’Key management’ supports, for example, ’encryption’.
- employedAt, to specify at what time of execution it is used (Runtime, compiletime, etc.)
- isProtectedBy, in this case it is an asset property that intersects with the security measures, also considered assets, with the relationship Asset -> isProtectedBy -> SecurityMechanism, this will also be useful to identify all the countermeasures used to protect an asset and consequently will be used in the calculation of the mitigated risk

From this we can deduce that this type of architecture allows to describe each countermeasure with properties that detail its functioning and applicability, as well as improving interoperability with other security frameworks and risk assessment tools, making the ontology usable for decision support in real ICT environments.

An additional benefit of this approach is the increased flexibility in managing updates. Since the cyber threat landscape is constantly evolving, a model that explicitly represents countermeasures allows for easy addition of new mitigation technologies without having to completely redefine the ontological structure. For example, the introduction of a new cryptographic standard such as Post-Quantum Cryptography could be handled by simply adding a new subclass of Encryption, while maintaining consistent relationships with existing assets and threats.

### 4.5.3 N-ary relations class and Usage

As previously stated, our ontology is implemented in OWL (Web Ontology Language) which is a description-logic based Language based on RDF, this allows to express only binary relations of the type: (subject, predicate, object), for example "Threat" isEnabledBy "Vulnerability". N-ary type relations such as "a **security mechanism** protects a **security goal** and an **asset** with a given **defense strategy**" cannot be expressed natively and to solve this problem it is necessary to introduce the use of a helper class[26].

This class works as bridge between all the related entities defining a link between itself and each of the entities considered. For example, in the case of a relation of type "students A took the exam B in date C" we can create a helper class, i.e. TakenExam, and link that to

al the related class involved, so "TakenExam" hasEsam "Exam", "TakenExam" hasStudent "Student", "TakenExam" inDate "Date".

The class, defined in the ontology as "NaryRelation", defines defense strategy, asset type and security goal allowing to define the properties used by the security mechanisms. In particular, the exclusive "protects" properties ("only") will be those that will be used later by the tool for the inference of the mitigated score.

This type of property, unlike the "some"(someValuesFrom) ones that serve to state that security mechanism1 protects at least the security property1, declare that the security measure in the best of cases protects the combination of the specified factors, excluding those untreated factors that "protects some" would not exclude.

For example, in the definition of VulnerabilityScanner, it is specified that this mechanism protects at least the integrity and correctness of a host using the detection strategy, thanks to the property:

restriction(protects someValuesFrom(*_Correctness*))
restriction(protects someValuesFrom(*_Host*))
restriction(protects someValuesFrom(*_Detection*))
restriction(protects someValuesFrom(*_Integrity*))

The use of someValuesFrom implies that there is at least one instance of the protects property that links VulnerabilityScanner to the _Correctness, _Integrity, _Host, and _Detection elements. However, this restriction does not prevent the mechanism from also protecting other resources or security objectives.

To ensure that the VulnerabilityScanner is not misinterpreted as a countermeasure protecting other properties (for example, a user's privacy), we use allValuesFrom, which constrains the values of the protects property to only the declared elements:

restriction(protects allValuesFrom(intersectionOf(unionOf(*_Correctness*
*_Integrity*) *_Host* unionOf(*_Detection _Correction*))))

This expression ensures that all protections offered by a VulnerabilityScanner are limited to the integrity or correctness of a host, using only detection or correction strategies.

The developed tool will take into account only the "AllValuesFrom" properties to define, in the "protects" property, the related entity to each of the security mechanism.

### Class Structure

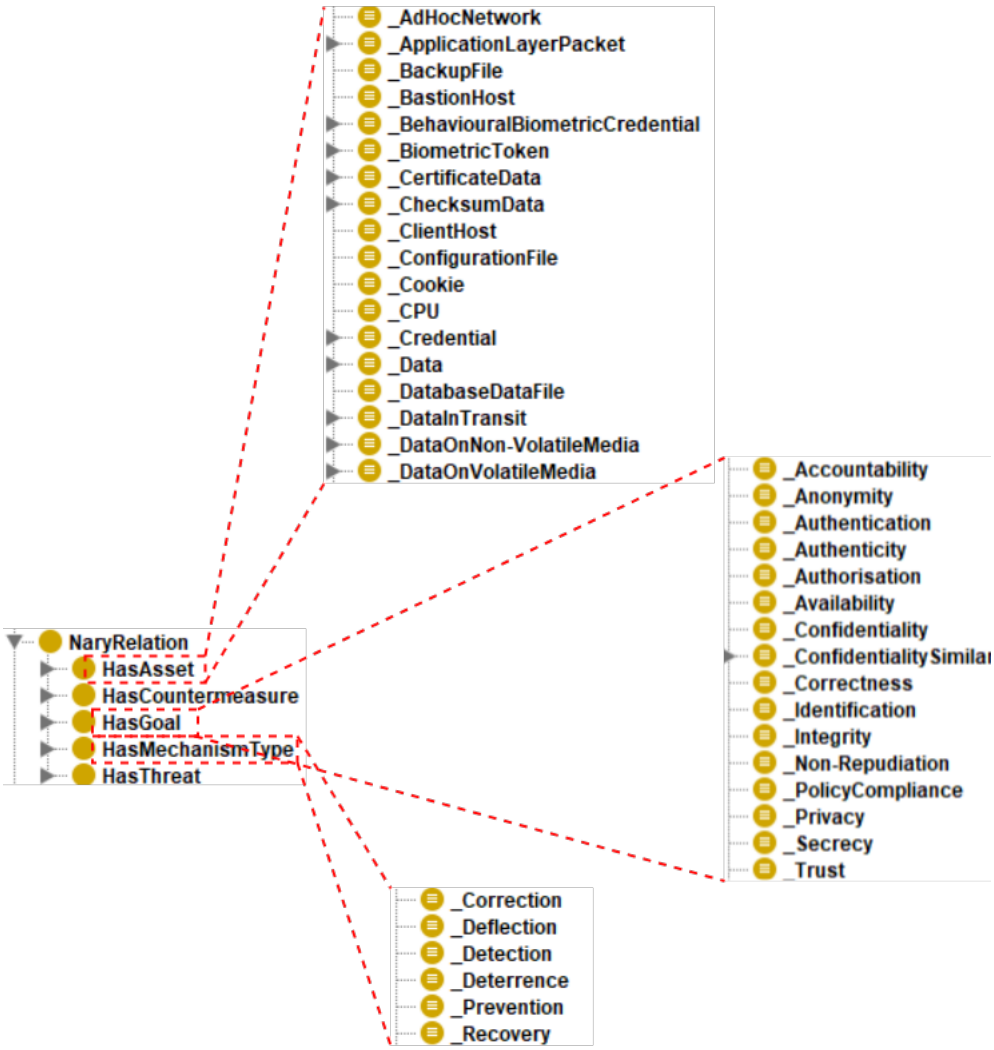


Figure 4.4. N-ary relation class in Protégé

The class (depicted in Figure 4.4 is composed of 5 sublasses, two of which were used in Herzog's work to perform queries to the ontology but, being useless for our purposes, will not be discussed, while the other 3 subclasses represent the following concepts:

- hasAsset, provides a detailed taxonomy that allows to accurately describe the asset under consideration
- hasGoal, represents the security properties that the countermeasure mitigates and the most important instances of this class are for example Confidentiality, Integrity,

Availability and Authentication and some of these are linked to each other, for example Privacy is linked to the Confidentiality, Anonimity and Trust properties.

- hasMechanismType, describes the type of security that is obtained by implementing a certain mitigation, the subclasses are prevention, detection, recovery, correction, deterrence and deflection.

## 4.6 Mitigated Score Calculation

During the decision process of how to calculate the risk, a wide research of the approaches proposed in the literature was done in order to evaluate the solutions already present. However, these possible solutions were poorly suited to our needs because in the case in which the infrastructure for which we wanted to make a risk assessment had not actually been implemented, the only proposed solutions were strongly dependent on the expert's knowledge, while our goal was to propose one that, gave the expert the possibility to adapt it, but was also, if required, independent from it and deterministic in the risk calculation. Instead, for those that had a practical implementation of the infrastructure, they used parameters derived from the network itself as input for the risk calculation operation, which in our case was not possible. So in the end we opted to propose a new solution presented below.

### 4.6.1 Experimental ideas

Initially it was clear that the factors that had to be considered for the calculation of the residual risk were the asset considered, the countermeasures that protected it and the threat that threatened it, but it was not clear how to actually conduct this operation, so several possible solutions were explored, presented below:

- The first involved recalculating the CVSS considering the change in parameters given by the mitigations and then reporting this reduction in the risk score, this solution, in addition to being difficult to apply since obtaining which parameters for the calculation of the CVSS had to be modified and by how much depending on the security mechanism was not an immediate task, did not even correctly reflect how much the mitigation had an effect because risk and vulnerability are two different concepts for which the risk score is calculated differently. For example, an asset could have 30 vulnerabilities all more or less mitigated by a mitigation mechanism, but only one with a very low ease of exploit and high availability would have been enough to theoretically leave the risk score unchanged, even if perhaps considering it partially mitigated thanks to the other vulnerabilities. For these reasons, this solution was discarded from the start.
- The second solution consisted in using a categorization of CAPECs in the ontology so as to be able to relate which security mechanisms protected which categories of CAPECs. To do this, the categorization had to ensure that a CAPEC could be linked to one and only one category and that these categories were divided in such a way as to represent the threatened security properties. This solution was also subsequently

discarded even though it was conceptually more correct because, given that even the categorization was not an easy task, it was thought for this solution to use the division of [26], however this was conceptually much closer to the concept of attack rather than risk and in fact for example some risks could be mapped on different categories of Herzog such as the CAPEC 510 "saas user request forgery" where in the description specifies that it can be obtained with a malware but not being the only option this CAPEC would be mappable on different categories of Herzog, in addition to then having to find a correlation with the security measures, for these reasons it was then established that this solution was not suitable for our purposes.

- The third and last, which will be the one then used, involved relating the consequences field of the CAPEC with the properties of the security mechanisms. Below is a more in-depth discussion.

### 4.6.2 Proposed Solution

The solution finally adopted involved the use of the consequences field of CAPEC, which represented the consequences in the event that a threat occurred in terms of violated security property and was organized as a vector of [11]:

- scope, represented the security property
- impact, described the type of impact in the event of the threat occurring
- note, provided a more detailed additional description and was optional

Considering this, the tool extracts the infrastructure assets and their type and from each of them obtains the associated security measures, then traces the class of these countermeasures and extracts the property that models the mitigation rule. In this rule, which is defined thanks to the use of the NaryRelation class, a combination of asset type, defense strategy and security goal, the tool will take care of replacing the real values and evaluating the overall expression in order to obtain a resulting mitigation factor. For example, if we had the asset "OS2" of the "_Process" type and this was protected by an instance of the "Antivirus" class whose "protects" property is: "protects only (_Technology and (_Availability or _Integrity or _PolicyCompliance) and (_Detection or _Prevention or _Recovery))" and _Process was a child class of _Technology, for the CAPEC "subverting environmental variable values" which has the following consequences: availability, confidentiality, authorization and accountability, for an initial risk of 20 it would be mitigated with a risk of 15 because by replacing the values in the expression, considering the logical "or" as sum operations and the "and" as products and considering that we are interested in all the defense strategies, we will obtain: "(1 * (0.25 + 0 + 0) * (0.33 + 0.33 + 0.33))".

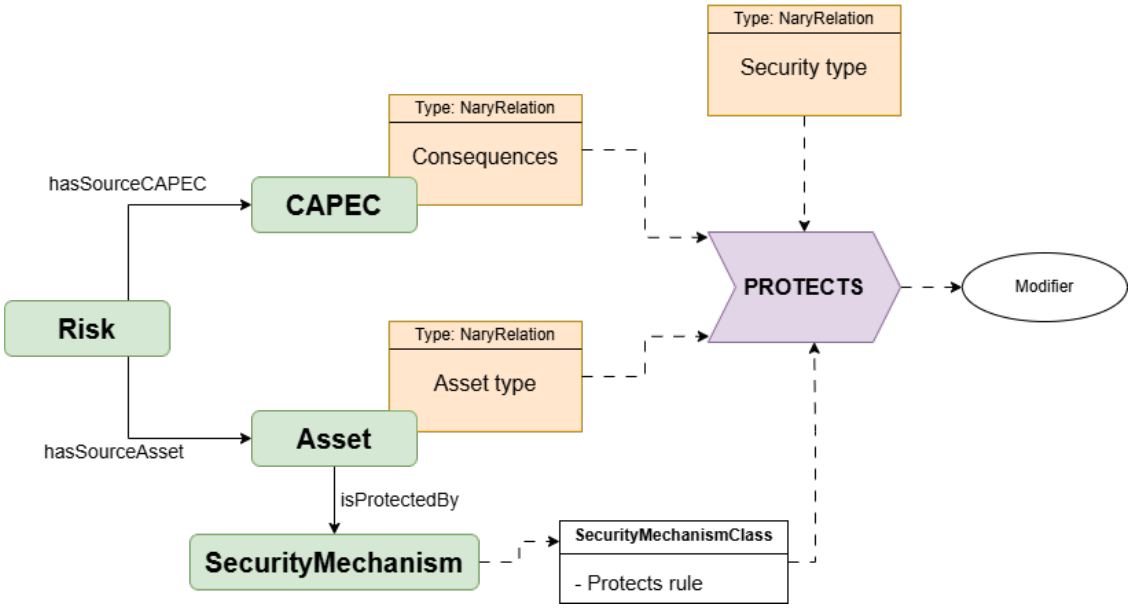


Figure 4.5. Data flow of the function

```
risk = search_for_risk(asset, CAPEC)
if risk exists:
  add_vuln(risk, vuln)
else:
  risk = new_risk(asset, CAPEC, vuln)

dict_def_strategy = new_dict_def_strategy()
dict_asset_type = new_dict_asset_type_by_asset(asset)
if (!CAPEC.consequences or !asset.isProtectedBy):
  exit

dict_sec_goal = new_dict_sec_goal()
assign_weight_by_consequences(dict_sec_goal)

if len(asset.isProtectedBy) > 0:
  modifier = 1
  for secMec in asset.isProtectedBy:
    protects = extract_protects_property(secMec)
    assign_weight_by_property(dict_def_strategy, protects)
    input=dict_def_strategy + dict_asset_type + dict_sec_goal
    expression = combine_expr(protects, input)
    score = eval(expression)
```

```
    modifier *= score

  if firewall in asset.isProtectedby:
    modifer = str(modifier) + "*"
  add_modifier_to_risk(risk, modifier)
  print(risk)
```

The function, called immediately after the vulnerability has been created, takes care of creating the instances of the risk class and populating them with the asset and the corresponding CAPEC, if there is not already an instance with this combination (search_for_risk(asset, CAPEC)), also reporting the vulnerability from which it was obtained. If the risk already exists, it is only connected to the vulnerability under consideration (add_vuln(risk, vuln)), otherwise a new instance is created (new_risk(asset, CAPEC, vuln)). Subsequently, the tool extracts from the ontology all the information it will need to calculate the risk and uses it to build the input to give to the function, including:

- obtains which NaryRelation class the asset is an instance of
- obtains the security mechanisms connected to the asset and consequently their "protects" rules (extract_protects_property(secMec))

Thanks to this information, it builds the three input dictionaries used for the evaluation:

- asset type dictionary (new_dict_asset_type_by_asset(asset)), where the keys are all the asset types obtained from NaryRelation that belong to the hierarchy of the asset considered, in this dictionary it is not necessary to divide the score into the various assets that compose it because it is assumed that in the "protecs" rules there is at most one asset type of each "hierarchy" of NaryRelation.
- defense strategy dictionary (new_dict_sec_goal()), this dictionary allows you to select which defense strategies are searched for by assigning them a value other than zero and subsequently this value will be replaced with the correct weight, depending on how many of these strategies are present in the rule used.
- security type dictionary (assign_weight_by_property(dict_def_strategy, protects)), which assigns to each type of security searched present in the consequences of the CAPEC a value equal to 1/the cardinality of the consequences of CAPEC. During the population of this dictionary, the concept of "Access Control", used in CAPEC, is also mapped to that of "Authorization", used instead by [26], in line with the definition of Access Control of the NIST which considers them synonyms: "The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances)" [38].

Subsequently, the function extracts all the security mechanisms of the asset in question, traces their class and obtains the corresponding "protects only" property. At this point the function can use a regular expression to convert the expression (combine_expr(protects, input)) and then evaluate the final value used as a mitigation factor for the score (eval(expression)) and saved in the Risk class of the ontology (add_modifier_to_risk(risk, modifier)). It

should also be noted that if the security mechanism is a firewall, the mitigated score will be reported with an asterisk in the ontology, to indicate that this may not completely reflect the practice. This is because, for example, if a web application were hosted on a server, it would be subject to CAPEC-6 argument injection which, among other consequences, also has confidentiality and integrity, properties that in theory the firewall should protect according to the rule used. However, unless the firewall was a WAF (web application firewall), it would not be able to block the payload of a sql injection and therefore the tool would erroneously mark the corresponding score as mitigated. In addition, the dataflow should also be taken into account and therefore what the origin of an attack could be, because in this case the firewall would be able to protect from an attack originating from the outside but not if this were internal. For these reasons, a possible extension of the tool could include the modeling of one or more metrics that somehow represent the effectiveness of the measure, in order to take these factors into account.

# Chapter 5

# Results and Considerations

In this chapter, the results obtained from the tool developed during our thesis will be presented and analyzed, highlighting both the strengths and the critical issues encountered. The main objective is to apply a real use case to the implemented model in order to evaluate the actual effectiveness of the proposed solution, underlining and proposing possible improvements to factors already present but which, due to limitations of the technologies used, could further improve the tool's output.

The results obtained in the work [12] will be extended, in whose development they were presented divided into three macro sections: during the threat modelling phase, the results of the swrl rules representing the risks associated with each asset and categorized into STRIDE categories are presented, in the vulnerability assessment phase instead it is reported the results of the query of public sources, limiting itself only to the most recent CVEs to provide a current and relevant vision, finally with the risk assessment phase it is presented the results quantifying the risks associated with the various CAPECs, providing a detailed overview of the security posture of the infrastructure.

The results highlight both the effectiveness of the proposed approach and some limitations related to the quality of data available in public databases.

## 5.1 Modified ICT Infrastructure

In Figure 5.1 is presented the infrastructure model used for validating the proposed solution.

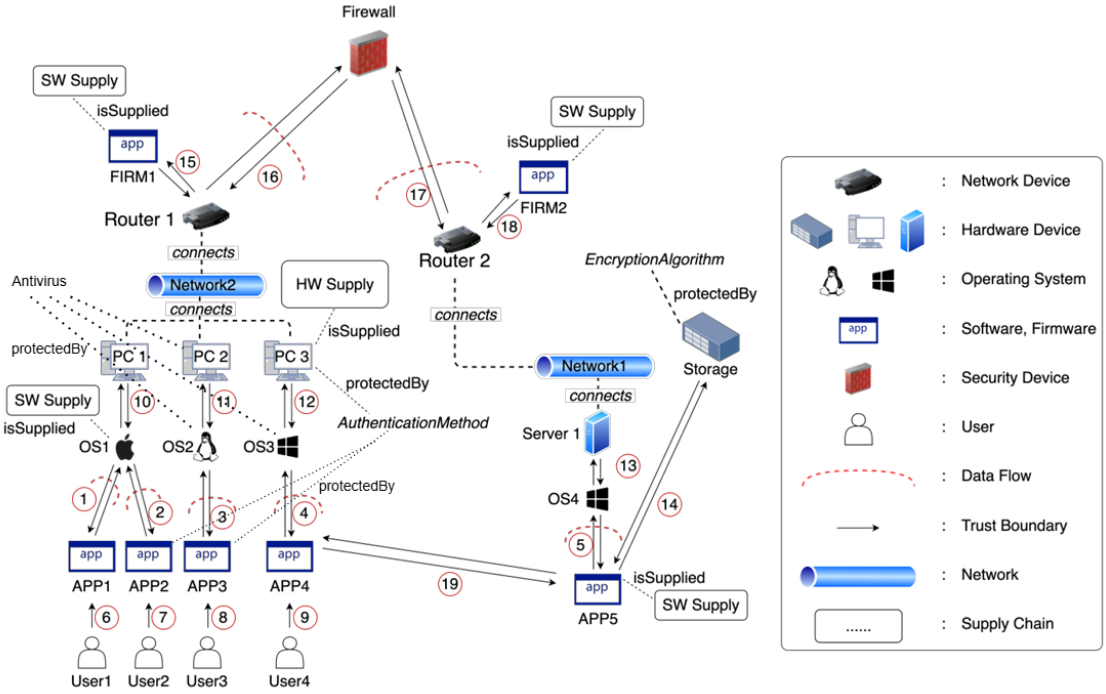


Figure 5.1. Diagram of the modified ICT infrastructure employed to evaluate the tool

The proposed architecture is a modified version of the one presented in [15] to integrate and represent the added ontological concepts. Before the modifications, the security mechanisms used were represented only by an authentication mechanism in relation to PC3, encryption algorithm for storage protection and a firewall. During the development of the thesis these protection measures were extended to:

- authentication mechanism, extended to app2, app3
- antivirus, applied to os2, os3, pc2
- firewall, applied to all hosts belonging to the subnets including router1 and network2

In addition to this, in order to allow the tool to correctly perform its inferences, the following NaryRelation classes were applied to the following assets:

- app -> "_process"
- dataflow -> "_dataInTransit"
- firewall -> "_bastionHost"
- firmware -> "_process"

- hardware supply -> "_hardware"
- network -> "_network"
- operating system -> "_process"
- pc -> "_hostOnIntranet"
- router -> "_router"
- server -> "_serverHost"
- storage -> "_stationaryData"
- software supply -> "_programFile"
- user -> "_human"
- antivirus -> "_process"

As for all those security measures that are not applied directly to an asset, but are assets themselves that somehow affect the security of other resources in the network, it is left to the security expert to establish which other assets they affect by modeling it in the ontology through the "isProtectedBy" property. Initially, it was thought to make this inference automatic, but later it was considered that deriving rules to establish whether an asset was protected or not, for example, by a firewall depending on the network topology was a task too difficult and too susceptible to errors that would have led to an incorrect risk assessment, compared to manually completing the work. Examples of security mechanisms of this type obtained during the thesis are: Firewall, IntrusionDetectionSystem, Onion-Router, Remailer, VPN (Virtual Private Network) and Network Address Translation.

## 5.2 Vulnerability Assessment

At the moment the instances of the vulnerability class are populated with CVE, CWE and ATT&CK, of which its techniques are linked to the various mitigation through the "hasMitigation" relation. During our work, as previously mentioned, the mitigation used have been expanded by enlarging this set to those of D3FEND. Below, we will report the results of the vulnerability assessment improved with the information of D3FEND.

### Vulnerabilities for APP3

1. **CVE**: CVE-2023-6206
   - **CVSS**: 5.4
   - **CWEs**: CWE-1021
   - **CAPECs**: CAPEC-181, CAPEC-504, CAPEC-654, CAPEC-506, CAPEC-587, CAPEC-103, CAPEC-222
   - **ATT&CKs -> D3FENDs**: T1036.004 -> {D3-SJA}, T1056, T1548.004 -> {D3-SCP, D3-DI, D3-RD, D3-SCF, D3-SCA}

## Vulnerabilities for OS1

2. **CVE**: CVE-2021-30693

   - **CVSS**: 7.8
   - **CWEs**: CWE-20
   - **CAPECs**: CAPEC-45, CAPEC-209, CAPEC-13, CAPEC-9, CAPEC-80, CAPEC-72, CAPEC-52, CAPEC-64, CAPEC-109, CAPEC-88, CAPEC-24, CAPEC-28, CAPEC-261, CAPEC-120, CAPEC-588, ...
   - **ATT&CKs -> D3FENDs**: T1562.003 -> {D3-ACH, D3-FIM, D3-CI, D3-EDL, D3-RC, D3-EFA, D3-RKD, D3-LFP, D3-FA, D3-RF, D3-EAL, D3-DF, D3-DA, D3-FEV, D3-FE}, T1027, T1036.001 -> {D3-DF, D3-EFA, D3-FE, D3-DA, D3-FIM, D3-FA, D3-LFP, D3-RF, D3-EDL, D3-EAL, D3-FEV}, T1574.007 -> {D3-FA, D3-DA, D3-EFA, D3-LFP, D3-RF, D3-FIM, D3-EDL, D3-EAL, D3-FE, D3-FEV, D3-DF}, ...

## Vulnerabilities for OS2

3. **CVE**: CVE-2023-45866

   - **CVSS**: 6.3
   - **CWEs**: CWE-287
   - **CAPECs**: CAPEC-633, CAPEC-151, CAPEC-194, CAPEC-650, CAPEC-593, CAPEC-115, CAPEC-94, CAPEC-114, CAPEC-22, CAPEC-57
   - **ATT&CKs -> D3FENDs**: T1040 -> {D3-DNSTA}, T1134, T1185 -> {D3-NTF, D3-RTSD, D3-NTCD, D3-UGLPA, D3-CSPP, D3-PHDURA, D3-NTSA, D3-PMAD}, T1505.003 -> {D3-PLM, D3-EFA, D3-LLM, ...}, T1563 -> {D3-RTSD, D3-ST, D3-NTF, ...}, ...

As mentioned in the Chapter 4.2 this solution currently allows to have an additional source from which to have a description of the possible mitigation usable against the attack associated with the vulnerability considered. A possible improvement would be to directly link the information related to both attacks and mitigation to the infrastructure without the intermediate step of vulnerabilities in order to have a more reliable and complete modeling. In this way, mitigation could be used both to model the security mechanisms already present, and as an output of the framework in the form: "considering the following infrastructure under consideration, the inferences indicate that this would be the set of possible attacks and consequently this is the set of possible countermeasures to mitigate the attacks obtained". Once this is done, the tool could be further extended, implementing an algorithm for the search of the minimum in order to minimize the costs of implementing the countermeasures while respecting the imposed limitations.

| Resource | CPE | Vendor | Product | Version |
|---|---|---|---|---|
| APP1 | cpe:2.3:a:apple:numbers:*:*:*:*:*:mac_os_x:*:* | MISSING | MISSING | MISSING |
| APP2 | cpe:2.3:a:apple:safari:14.0:*:*:*:*:*:*:* | MISSING | MISSING | MISSING |
| APP3 | cpe:2.3:a:mozilla:thunderbird:101.0:*:*:*:*:*:*:* | MISSING | MISSING | MISSING |
| APP4 | cpe:2.3:a:microsoft:sql_server_management_studio:*:*:*:*:*:*:*:* | MISSING | MISSING | MISSING |
| APP5 | cpe:2.3:a:microsoft:sql_server:2022:*:*:*:*:*:x64:* | MISSING | MISSING | MISSING |
| FIRM1 | cpe:2.3:o:tp-link:tl-er7520g_firmware:-:*:*:*:*:*:*:* | MISSING | MISSING | MISSING |
| FIRM2 | cpe:2.3:o:dlink:dsr-250n_firmware:3.17:*:*:*:*:*:*:* | MISSING | MISSING | MISSING |
| Firewall1 | cpe:2.3:o:sophos:sfos:18.0:*:*:*:*:*:*:* | MISSING | MISSING | MISSING |
| Network1 | MISSING | MISSING | MISSING | MISSING |
| Network2 | MISSING | MISSING | MISSING | MISSING |
| OS1 | cpe:2.3:o:apple:mac_os_x:10.14:*:*:*:*:*:*:* | MISSING | MISSING | MISSING |
| OS2 | cpe:2.3:o:canonical:ubuntu_linux:22.04:*:*:*:lts:*:*:* | MISSING | MISSING | MISSING |
| OS3 | cpe:2.3:o:microsoft:windows_11_22h2:*:*:*:*:*:*:x64:* | MISSING | MISSING | MISSING |
| OS4 | cpe:2.3:o:microsoft:windows_server_2022:10.0.20348.1547:*:*:*:azure:*:x64:* | MISSING | MISSING | MISSING |
| PC1 | MISSING | MISSING | MISSING | MISSING |
| PC2 | MISSING | dell | alienware_13_r2 | MISSING |
| PC3 | MISSING | MISSING | MISSING | MISSING |
| Router1 | MISSING | MISSING | MISSING | MISSING |
| Router2 | MISSING | MISSING | MISSING | MISSING |
| Server1 | MISSING | dell | poweredge_t440 | MISSING |
| Storage | MISSING | MISSING | MISSING | MISSING |

Figure 5.2. CPE of the analyzed asset [12]

## 5.3 Threat modeling

The threat modelling process was performed through two distinct workflows in order to compare the results obtained and evaluate the effectiveness of the two solutions:

BRON Workflow: in this solution the report produced contains about 400 results, of which a small set is presented in Table 5.1, the reason is to be found in the fact that the data is inferred from public security databases. In fact, first of all for all those assets for which the CPE is not modeled in the ontology it is impossible to obtain the threats (reported in Figure 5.2), furthermore it is well known that one of the biggest problems of these knowledge bases is the poor if not missing relationship between them. Therefore, by following the CPE -> CVE -> CWE -> CAPEC hierarchy, the information obtained gradually becomes thinner, causing the presence of false negatives, i.e. data that would have been correct to expect but that do not occur. The resolution of this problem, however, would require a shared effort by the industry community in order to improve these knowledge bases, making them more complete and reliable. To overcome this, the tool uses

a second mechanism to infer the threats that the assets are affected by that is independent of CPE and all of the aforementioned databases.

| Resource | Type | Threat | Risk | Risk Level |
|---|---|---|---|---|
| APP2 | Software | CAPEC-588 | 20 | Very High |
| APP2 | Software | CAPEC-67 | 20 | Very High |
| APP2 | Software | CAPEC-44 | 20 | Very High |
| APP2 | Software | CAPEC-75 | 20 | Very High |
| OS3 | OperatingSystem | CAPEC-100 | 20 | Very High |
| APP3 | Software | CAPEC-21 | 16 | High |
| OS1 | OperatingSystem | CAPEC-135 | 16 | High |
| OS2 | OperatingSystem | CAPEC-45 | 16 | High |
| OS2 | OperatingSystem | CAPEC-267 | 16 | High |
| OS3 | OperatingSystem | CAPEC-92 | 16 | High |
| APP3 | Software | CAPEC-160 | 12 | Medium |
| APP3 | Software | CAPEC-504 | 12 | Medium |
| OS1 | OperatingSystem | CAPEC-115 | 12 | Medium |
| OS1 | OperatingSystem | CAPEC-540 | 8 | Medium |

Table 5.1. Threat modeling results from BRON

ThreMA Workflow: Unlike the previous solution, this one uses rules implemented through the SWRL language to be able to infer, given the starting infrastructure modeled through the ontology and given the categorization of the CAPECs, directly which CAPECs threaten which assets. The report produced by this workflow produces about 10,000 results, of which again a small set is presented in Table 5.2. This is partly due to the fact that the assets considered are all and not just those with the cpe and partly due to the fact that the rules are less stringent than the database inferences and therefore many more CAPECs are associated with the same asset. This solution, being more conservative, tends to overestimate the associated risks producing more false positives, generating a number of threats that are not always relevant from an operational point of view. To improve this aspect, the threat modeling rules should be refined by considering additional factors in their definition.

The two previous tables show a subsection of the results obtained from the two workflows. Looking for the differences between the two, we can see that out of 377 results from bron, about 60% are also obtained in the same way from the inference rules. This missing 40% demonstrates even more how on the one hand a better refinement of the threat modeling rules and categorization of the CAPECs is needed. In fact, for example, the CAPEC-75 that is reported by the results deriving from bron linked to the asset "app2", is not reported in the results of the swrl rules because it is categorized in supply chain and not in software, while on the other hand the mapping through bron should also be improved by excluding all those CAPECs obtained from cwe with the mapping field "discouraged", as demonstrated by the case of the CAPEC-58 "restful priviledge elevation" erroneously correlated to an operating system (os3) type asset via CWE-269.

| Resource | Type | Threat | Risk | Risk Level |
|---|---|---|---|---|
| APP2 | Software | CAPEC-588 | 20 | Very High |
| APP2 | Software | CAPEC-67 | 20 | Very High |
| APP2 | Software | CAPEC-44 | 20 | Very High |
| OS2 | OperatingSystem | CAPEC-470 | 20 | Very High |
| OS3 | OperatingSystem | CAPEC-100 | 20 | Very High |
| OS1 | OperatingSystem | CAPEC-135 | 16 | High |
| APP3 | Software | CAPEC-21 | 16 | High |
| OS2 | OperatingSystem | CAPEC-45 | 16 | High |
| OS2 | OperatingSystem | CAPEC-267 | 16 | High |
| OS3 | OperatingSystem | CAPEC-92 | 16 | High |
| PC1 | HardwareDevice | CAPEC-402 | 16 | High |
| DF19-B | DataFlow | CAPEC-162 | 16 | High |
| FIRM1 | Firmware | CAPEC-240 | 16 | High |
| APP3 | Software | CAPEC-160 | 12 | Medium |
| APP3 | Software | CAPEC-504 | 12 | Medium |
| OS1 | OperatingSystem | CAPEC-115 | 12 | Medium |
| Firewall1 | Firewall | CAPEC-114 | 12 | Medium |
| Router2 | NetworkDevice | CAPEC-114 | 12 | Medium |
| OS3 | OperatingSystem | CAPEC-178 | 9 | Medium |
| APP3 | Software | CAPEC-121 | 8 | Medium |
| OS1 | OperatingSystem | CAPEC-540 | 8 | Medium |
| Network2 | Network | CAPEC-169 | 4 | Low |

Table 5.2. Threat modeling results from SWRL rules

The comparison between the two workflows allowed us to identify a trade-off between sensitivity and specificity in threat detection, suggesting the need to find a balance between the two proposed solutions.

## 5.4 Risk Assessment

In this section, the results of the risk assessment performed by Pyra as described in Section 4.6 will be reported with particular attention to the scores mitigated by the countermeasures.

In the risk assessment results obtained from bron we could find, with the described infrastructure, a number of mitigated risks equal to 101 out of 377. Many factors contributed to this result:

- first of all not all assets had associated countermeasures.
- as previously reported another factor was the fact that some CAPECs were missing the populated consequences field such as CAPEC-229 "Serialized Data Parameter Blowup" for the os2 asset.

| Resource | Type | Threat | Risk | Mitigated Risk | Risk Level |
|---|---|---|---|---|---|
| APP2 | Software | CAPEC-560 | 16 | 10.6 | Medium |
| APP2 | Software | CAPEC-600 | 16 | 10.6 | Medium |
| APP3 | Software | CAPEC-21 | 16 | 10.6 | Medium |
| Router1 | NetworkDevice | CAPEC-560 | 16 | 10.6 | Medium |
| OS3 | OperatingSystem | CAPEC-100 | 20 | 10 | Medium |
| OS2 | OperatingSystem | CAPEC-267 | 16 | 9.6 | Medium |
| OS3 | OperatingSystem | CAPEC-92 | 16 | 8 | Medium |
| OS3 | OperatingSystem | CAPEC-178 | 9 | 6.75 | Medium |
| OS2 | OperatingSystem | CAPEC-45 | 16 | 5.3 | Medium |
| APP3 | Software | CAPEC-121 | 8 | 5.3 | Medium |
| Firewall1 | Firewall | CAPEC-07 | 15 | 5 | Medium |
| Router1 | NetworkDevice | CAPEC-681 | 15 | 5 | Medium |
| Firewall1 | Firewall | CAPEC-74 | 12 | 4 | Low |
| PC2 | HardwreDevice | CAPEC-26 | 16 | 4.0 | Low |
| APP3 | Software | CAPEC-504 | 12 | 0 | Very Low |

Table 5.3. Risk assessment results

- as a last reason that obviously the security measures were not always suitable to mitigate certain types of CAPEC such as for example for CAPEC-44 "Overflow Binary Resource File" whose affected security properties are only availability, with app2 protected by firewall and authentication mechanism, is not mitigated or asset as for CAPEC-67 "String Format Overflow in syslog()" which has as possible consequences integrity and is connected to app3 that not being a host or data in transit are not protected by the firewall even if the firewall would protect those security properties.

Below, a series of examples will be presented that demonstrate in which cases the inferences obtained from the tool have proven useful:

- CAPEC-21 "Exploitation of Trusted Identifiers" for app2 which reports in the consequences authentication, confidentiality and integrity, protected by the authentication mechanism reports a percentage of mitigation equal to 33%, as reported in Table 5.4.

| | **Authentication Mechanism** | **Mitigation** |
|---|---|---|
| CAPEC-21<br>Consequences:<br>Authentication → Gain Privileges<br>Confidentiality → Read Data<br>Integrity → Modify Data | protects only (_Authentication and _Prevention and (_Human or _Technology)) | 33% |
| APP2<br>_Process | | |

Table 5.4. Risk assessment for CAPEC-21 and app2

- CAPEC 123 "Buffer Manipulation" for os3, threat availability and confidentiality, of which the second is protected by the antivirus resulting in a mitigation equal to 50%, as reported in Table 5.5.

| | **Authentication Mechanism** | **Mitigation** |
|---|---|---|
| CAPEC-123<br>Consequences:<br>Availability → Unreliable Executions<br>Confidentiality → Read Data | protects only (_Technology and (_Availability or _Integrity or _PolicyCompliance) and (_Detection or _Prevention or _Recovery)) | 50% |
| OS3<br>_Process | | |

Table 5.5. Risk assessment for CAPEC-123 and os3

- CAPEC 127 "Directory Indexing" for pc2, threat confidentiality but, because it is a host in a network protected by a firewall, it is mitigated, as reported in Table 5.6.

| | **Authentication Mechanism** | **Mitigation** |
|---|---|---|
| CAPEC-127<br>Consequences:<br>Confidentiality → Read Data | protects only (_Prevention and ((_DataInTransit and _PolicyCompliance) or ((_Availability or _Confidentiality or _Integrity) and (_Host or _Intranet)))) | 100% |
| PC2<br>_HostOnIntranet | | |

Table 5.6. Risk assessment for CAPEC-127 and pc2

## 5.5 Considerations about Efficacy

During the implementation and evaluation of the proposed model, some critical issues and possible margins for improvement emerged. In this subsection, these factors found will be exposed to have a starting point from which to draw inspiration for the improvement of the model.

First of all, as also reported in the previous paragraph, it was found that out of 559 total CAPECs, 190 are missing information related to the consequences field, this does not allow the application of the ontology rules to calculate the mitigated risk. This lack is due to the fact, widely recognized in the sector, that these public knowledge bases often lack data and relationships, to overcome this problem, since manual methods would require considerable effort, new approaches based on machine learning have been proposed to automate the process of linking the various entities of the public databases [12].

Another determining factor in evaluating the effectiveness of the framework is the evaluation of the security properties actually used: in fact, to ensure that the modeling is complete, it is important to evaluate the sets of properties used by [26] and by CAPEC. The first one includes the security properties depicted in Figure 5.3 of which, however, only the following are actually used: Anonymity, Authentication, Availability, Confidentiality, Correctness, Integrity, Policy Compliance, Privacy and Trust.


Figure 5.3. Security goal of Nary relations

Instead, the security goals used in CAPEC entries are:

```
[
  "Access Control",
  "Accountability",
```

```
    "Authentication",
    "Authorization",
    "Availability",
    "Confidentiality",
    "Integrity",
    "Non-Repudiation",
    "Other",
]
```

From this data it is clear that the security goals that have an effective role in mitigation are exclusively: Authentication, Availability, Confidentiality, Integrity. From this evaluation it is clear the importance of reviewing both the rules of the security mechanisms and the properties used by [26] with the aim of adapting and conceptually aligning with the attributes used in CAPEC entries.

A particular example of this concerns the Authorization property which in [26] is scarcely used despite some security mechanisms explicitly referring to Access control including file and database access control. Browsing the ontology, we can see how these mechanisms protect confidentiality and integrity that can be considered the direct consequences of authorization. We can also see how authentication is largely more used in contexts where authorization would also be related. From this, we can deduce that an improvement in the modeling of the properties or a hierarchization of these would allow a more accurate evaluation of the security posture of the infrastructure.

Finally, another possible point of improvement could be to give the security expert the possibility to customize the inputs used by the system to obtain the mitigated risk score. This is already possible, even if in a not very user-friendly way, for security types, while it would be even more flexible if it were also implemented for security goals. Taking as an example the case of a system, let's think of a public list of revoked digital certificates protected by a fileAccessControl mechanism, for which the expert needs to protect the integrity of the data he uses but is not interested in confidentiality, it would be useful to be able to allow him to select the security objectives he is interested in so as to use this information in the rules of the security mechanisms to have a vision closer to personal needs.

# Chapter 6

# Conclusions and Future Work

During the development of this thesis we extended PyRA, an ontology-based tool for the risk assessment of an ICT infrastructure. Our work focused mainly on evaluating and applying the solutions proposed in the literature to model, in an effective and appropriate way for our purposes, the security measures that can be used by the system.

The changes made to the ontology have thus allowed us to implement a process for calculating the quantitative residual risk, automatic and innovative compared to the solutions proposed by current scientific articles, which takes into account the types of assets under examination, the types of security wanted and the security properties.

The main advantages offered by this approach lie in the possibility of supporting the security expert, reducing his workload, helping him in conducting the risk assessment process thanks to the automation provided by the framework that allows to replace all those work phases that are normally manual, obtaining timely results and supporting decisions regarding the allocation of resources for risk mitigation. In this regard, the possibility of taking into account the security measures present in the risk calculation allows for a better prioritization of the necessary countermeasures.

Furthermore, since the process itself is automatic, this allows for the provision of deterministic and objective results that are independent of the experience of the security expert, who can use, if necessary, the output of the tool as a starting point for further analysis. In fact, many situations still require a certain amount of versatility and this is achieved thanks to the possibility of adapting the parameters used based on individual needs.

In this regard, a future effort for the further development of the tool could include the improvement of the modeling of the metrics used to calculate the mitigated risk, such as the introduction of a factor that indicates the effectiveness of the measure, in addition to the improvement of the mechanisms for modifying the current ones. An expansion of the knowledge base would also be necessary to be able to provide a more complete view of the risk assessment result.

Another possible starting point for the evolution of the tool could come from the improvement of the modeling of security measures, currently very much linked to the physical infrastructure, could in the future also include all those "best practices" type measures, consequently including the human factor in the process.

In addition to this, the process could be further expanded to also consider the general conditions of the network for which we are carrying out the risk assessment, both with a

static approach such as specifying the most exposed network sections and more dynamic, integrating it with an operational infrastructure, so as to be able to use the data coming from the network monitoring sources to improve the accuracy of the assessments in real time.

To conclude, during the development of the thesis we explored an innovative approach for calculating the risk of an ICT infrastructure. Certainly further studies and improvements will be necessary to be able to consider the developed tool effective and of real help, however it represents an important first step for future developments and applications in the field of IT risk assessment.

# Bibliography


[1] Malina Adach, Kaj Hänninen, and Kristina Lundqvist. «Security ontologies: A systematic literature review». In: *International Conference on Enterprise Design, Operations, and Computing*. Springer. 2022, pp. 36–53.

[2] Vivek Agrawal. «Towards the Ontology of ISO/IEC 27005: 2011 Risk Management Standard.» In: *HAISA*. 2016, pp. 101–111.

[3] Khandakar Ashrafi Akbar, Fariha Ishrat Rahman, Anoop Singhal, Latifur Khan, and Bhavani Thuraisingham. «The Design and Application of a Unified Ontology for Cyber Security». In: *International Conference on Information Systems Security*. Springer. 2023, pp. 23–41.

[4] Mohammed Noraden Alsaleh, Ehab Al-Shaer, and Ghaith Husari. «Roi-driven cyber risk mitigation using host compliance and network configuration». In: *Journal of Network and Systems Management* 25.4 (2017), pp. 759–783.

[5] Mohammed Noraden Alsaleh, Ghaith Husari, and Ehab Al-Shaer. «Optimizing the RoI of cyber risk mitigation». In: *2016 12th International Conference on Network and Service Management (CNSM)*. 2016, pp. 223–227. DOI: 10.1109/CNSM.2016.7818421.

[6] Cristian Amancei. «Practical methods for information security risk management». In: *Informatica economica* 15.1 (2011), p. 151.

[7] Richard L Baskerville, Jongwoo Kim, and Carl Stucke. «The cybersecurity risk estimation engine: A tool for possibility based risk analysis». In: *Computers & Security* 120 (2022), p. 102752.

[8] Carlos Blanco, Joaquín Lasheras, Eduardo Fernández-Medina, Rafael Valencia-García, and Ambrosio Toval. «Basis for an integrated security ontology according to a systematic review of existing proposals». In: *Computer Standards & Interfaces* 33.4 (2011), pp. 372–388.

[9] Carlos Blanco, Joaquin Lasheras, Rafael Valencia-García, Eduardo Fernández-Medina, Ambrosio Toval, and Mario 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.

[10] Adam Boyer, Erdogan Dogdu, Roya Choupani, Jason S Watson, Diego Sanchez, and Alexander Ametu. «Toward a Unified Cybersecurity Knowledge Graph: Leveraging Ontologies and Open Data Sources». In: *Southwest Data Science Conference*. Springer. 2024, pp. 17–33.

[11] capec. *capec consequences*. [Online; Accessed 2025, 7 march]. URL: https://capec.mitre.org/documents/schema/index.html#ConsequencesType.

[12] Christian Casalini. «Development of an Ontology-based Tool for Risk Assessment Automation». PhD thesis. Politecnico di Torino, 2023.

[13] CIS. *A Measurement Companion to the CIS Critical Security Controls*. https://www.tml.org/DocumentCenter/View/70/Measurement-Companion-to-the-CIS-Critical-Security-Controls-PDF. [Online; Accessed 2025, 7 march]. 2015.

[14] Fabio De Rosa, Nicolò Maunero, Luca Nicoletti, Paolo Prinetto, Martina Trussoni, et al. «Ontology for Cybersecurity Governance of ICT Systems.» In: *ITASEC*. 2022, pp. 52–63.

[15] Fabio De Rosa, Nicolò Maunero, Paolo Prinetto, Federico Talentino, and Martina Trussoni. «ThreMA: Ontology-Based Automated Threat Modeling for ICT Infrastructures». In: *IEEE Access* 10 (2022), pp. 116514–116526. DOI: 10.1109/ACCESS.2022.3219063.

[16] Stelios Dritsas, Lazaros Gymnopoulos, Maria Karyda, Theodoros Balopoulos, Spyros Kokolakis, Costas Lambrinoudakis, and Stefanos Gritzalis. «Employing Ontologies for the Development of Security Critical Applications: The secure e-poll paradigm». In: *Challenges of Expanding Internet: E-Commerce, E-Business, and E-Government: 5 th IFIP Conference e-Commerce, e-Business, and e-Government (I3E'2005), October 28–30, 2005, Poznan, Poland*. Springer. 2005, pp. 187–201.

[17] Andreas Ekelhart, Stefan Fenz, Markus D Klemen, and Edgar R Weippl. «Security ontology: Simulating threats to corporate assets». In: *Information Systems Security: Second International Conference, ICISS 2006, Kolkata, India, December 19-21, 2006. Proceedings 2*. Springer. 2006, pp. 249–259.

[18] Golnaz Elahi, Eric Yu, and Nicola Zannone. «A modeling ontology for integrating vulnerabilities into security requirements conceptual foundations». In: *International Conference on Conceptual Modeling*. Springer. 2009, pp. 99–114.

[19] Arnau Erola, Ioannis Agrafiotis, Jason RC Nurse, Louise Axon, Michael Goldsmith, and Sadie Creese. «A system to calculate Cyber Value-at-Risk». In: *Computers & Security* 113 (2022), p. 102545.

[20] Arnau Erola, Louise Axon, Alastair Janse van Rensburg, Ioannis Agrafiotis, Michael Goldsmith, and Sadie Creese. «Control effectiveness: A capture-the-flag study». In: *Proceedings of the 16th International Conference on Availability, Reliability and Security*. 2021, pp. 1–10.

[21] esentire. *Cybersecurity Ventures Report on Cybercrime*. https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime. [Online; Accessed 2025, 7 march]. 2024.

[22] exabeam. *What Is MITRE D3FEND?* https://www.exabeam.com/explainers/mitre-attck/what-is-mitre-d3fend/. [Online; Accessed 2025, 7 march].

[23] Stefan Fenz and Andreas Ekelhart. «Formalizing information security knowledge». In: *Proceedings of the 4th international Symposium on information, Computer, and Communications Security*. 2009, pp. 183–194.

[24] Jian-bo Gao, Bao-wen Zhang, Xiao-hua Chen, and Zheng Luo. «Ontology-based model of network and computer attacks for security assessment». In: *Journal of Shanghai Jiaotong University (Science)* 18 (2013), pp. 554–562.

[25] Sanjay Goel and Vicki Chen. «Information security risk analysis-a matrix-based approach». In: *Proceedings of the Information Resource Management Association (IRMA) International Conference*. 2005, pp. 1–9.

[26] Almut Herzog, Nahid Shahmehri, and Claudiu Duma. «An ontology of information security». In: *International Journal of Information Security and Privacy (IJISP)* 1.4 (2007), pp. 1–23.

[27] Chiao-Cheng Huang, Pei-Yu Huang, Ying-Ren Kuo, Guo-Wei Wong, Yi-Ting Huang, Yeali S. Sun, and Meng Chang Chen. «Building Cybersecurity Ontology for Understanding and Reasoning Adversary Tactics and Techniques». In: *2022 IEEE International Conference on Big Data (Big Data)*. 2022, pp. 4266–4274. DOI: 10.1109/BigData55660.2022.10021134.

[28] Douglas W Hubbard and Richard Seiersen. *How to measure anything in cybersecurity risk*. John Wiley & Sons, 2023.

[29] Peter E Kaloroumakis and Michael J Smith. «Toward a knowledge graph of cybersecurity countermeasures». In: *The MITRE Corporation* 11 (2021), p. 2021.

[30] Georgios Kavallieratos, Georgios Spathoulas, and Sokratis Katsikas. «Cyber risk propagation and optimal selection of cybersecurity controls for complex cyberphysical systems». In: *Sensors* 21.5 (2021), p. 1691.

[31] Ahmed Khan, Jeremy Bryans, and Giedre Sabaliauskaite. «Framework for calculating residual cybersecurity risk of threats to road vehicles in alignment with ISO/SAE 21434». In: *International Conference on Applied Cryptography and Network Security*. Springer. 2022, pp. 235–247.

[32] Masoud Khosravi-Farmad and Abbas Ghaemi-Bafghi. «Bayesian decision network-based security risk management framework». In: *Journal of Network and Systems Management* 28 (2020), pp. 1794–1819.

[33] Anya Kim, Jim Luo, and Myong Kang. «Security ontology for annotating resources». In: *On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE: OTM Confederated International Conferences, CoopIS, DOA, and ODBASE 2005, Agia Napa, Cyprus, October 31-November 4, 2005, Proceedings Part II*. Springer. 2005, pp. 1483–1499.

[34] Sasawat Malaivongs, Supaporn Kiattisin, and Pattanaporn Chatjuthamard. «Cyber trust index: A framework for rating and improving cybersecurity performance». In: *Applied Sciences* 12.21 (2022), p. 11174.

[35] mitre. *defend mitre faq*. https://d3fend.mitre.org/faq/. [Online; Accessed 2025, 7 march].

[36] Bruno Augusti Mozzaquatro, Carlos Agostinho, Diogo Goncalves, João Martins, and Ricardo Jardim-Goncalves. «An ontology-based cybersecurity framework for the internet of things». In: *Sensors* 18.9 (2018), p. 3053.

[37] NIST. https://csrc.nist.gov/glossary/term/risk_assessment. [Online; Accessed 2025, 7 march].

[38] nist. *access control definition*. https://csrc.nist.gov/glossary/term/access_control. [Online; Accessed 2025, 7 march].

[39] Jonathan Pagett and SL Ng. «Improving residual risk management through the use of security metrics». In: *Royal Holloway Series* (2010).

[40] Jakub Pastuszuk, Patryk Burek, and Bogdan Księżopolski. «Cybersecurity ontology for dynamic analysis of IT systems». In: *Procedia Computer Science* 192 (2021), pp. 1011–1020.

[41] Teresa Susana Mendes Pereira and Henrique M Dinis Santos. «An Ontology Approach in Designing Security Information Systems to Support Organizational Security Risk Knowledge.» In: *KEOD*. 2012, pp. 461–466.

[42] Nayot Poolsappasit, Rinku Dewri, and Indrajit Ray. «Dynamic Security Risk Management Using Bayesian Attack Graphs». In: *IEEE Transactions on Dependable and Secure Computing* 9.1 (2012), pp. 61–74. DOI: 10.1109/TDSC.2011.34.

[43] Simona Ramanauskaitė, Dmitrij Olifer, Nikolaj Goranin, and Antanas Čenys. «Security ontology for adaptive mapping of security standards». In: (2013).

[44] Markus Schumacher and Markus Schumacher. «6. toward a security core ontology». In: *Security Engineering with Patterns: Origins, Theoretical Model, and New Applications* (2003), pp. 87–96.

[45] shellsharks. *The Enchiridion of Impetus Exemplar*. https://shellsharks.com/threat-modeling. [Online; Accessed 2025, 7 march]. 2022.

[46] Amina Souag, Camille Salinesi, and Isabelle 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.

[47] Candace Suh-Lee and Juyeon Jo. «Quantifying security risk by measuring network risk conditions». In: *2015 IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS)*. 2015, pp. 9–14. DOI: 10.1109/ICIS.2015.7166562.

[48] Zareen Syed, Ankur Padia, M Lisa Mathews, Tim Finin, Anupam Joshi, et al. «UCO: A unified cybersecurity ontology». In: *Proceedings of the AAAI Workshop on Artificial Intelligence for Cyber Security*. 2016, pp. 195–202.

[49] B. Tsoumas and D. Gritzalis. «Towards an Ontology-based Security Management». In: *20th International Conference on Advanced Information Networking and Applications - Volume 1 (AINA'06)*. Vol. 1. 2006, pp. 985–992. DOI: 10.1109/AINA.2006.329.

[50] Bill Tsoumas, Stelios Dritsas, and Dimitris Gritzalis. «An ontology-based approach to information systems security management». In: *International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security*. Springer. 2005, pp. 151–164.

[51] Jeffrey Undercoffer, Anupam Joshi, and John Pinkston. «Modeling computer attacks: An ontology for intrusion detection». In: *International Workshop on Recent Advances in Intrusion Detection*. Springer. 2003, pp. 113–135.

[52] Jiali Wang, Martin Neil, and Norman Fenton. «A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model». In: *Computers & Security* 89 (2020), p. 101659.

[53] Ju An Wang and Minzhe Guo. «OVM: an ontology for vulnerability management». In: *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies*. 2009, pp. 1–4.