University of Zurich^UZH

MASTER THESIS – Communication Systems Group, Prof. Dr. Burkhard Stiller

Toward Collaborative and Cooperative Cybersecurity: A Survey on Approaches, Challenges, and Opportunities

Flavia Fulea
Zürich, Switzerland
Student ID: 17-724-345

Supervisor: Jan von der Assen, Christian Killer
Date of Submission: August 24, 2022

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland

ifi

Master Thesis
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland
URL: http://www.csg.uzh.ch/

Abstract

Cyberattacks are posing a threat to the continuity and success of organisations worldwide [1] and the costs associated with cybersecurity skyrocketed in the last years, reaching USD 6.9 billion in 2021 [2]. Therefore, the need for appropriate cybersecurity has never been higher. While malicious parties are teaming up to collaborate and cooperate on attacks, it is only natural that defenders should also cooperate or collaborate with each other in order to detect vulnerabilities or mitigate attacks. Firstly, this work gives an overview of the current state of cybersecurity and important concepts, and frameworks are discussed. Subsequently, definitions for collaborative cybersecurity and cooperative cybersecurity are proposed. A taxonomy is presented that could serve as a good categorisation basis for the existing research. A survey of the literature is performed, leveraging the proposed taxonomy. Finally, key limitations, trends and challenges are identified. As shown, current approaches focus on vulnerabilities sharing, intrusion detection and access control. While challenges remain with regards to the right amount of transparency in cybersecurity and to public-private cybersecurity collaboration and cooperation.

Kurzfassung

Cyberangriffe gefährden die Kontinuität und den Erfolg von Unternehmen weltweit [1]. So sind in den letzten Jahren die mit Cybersicherheit verbundenen Kosten auf 6,9 Milliarden US-Dollar gestiegen [2]. Folglich ist der Bedarf an angemessener Cybersicherheit so gross wie nie zuvor. Böswillige Parteien schliessen sich immer öfter zusammen, um bei Angriffen zu kollaborieren und kooperieren, daher erscheint es sinnvoll, dass auch Verteidiger sich zusammenschliessen, um gemeinsam Schwachstellen zu erkennen oder Angriffe abzuschwächen. Zunächst gibt diese Arbeit einen Überblick über den aktuellen Stand der Cybersicherheit und diskutiert wichtige Konzepte und Rahmenbedingungen. Anschliessend werden Definitionen für kollaborative Cybersicherheit und kooperative Cybersicherheit formuliert. In einem weiteren Schritt wird eine Taxonomie aufgestellt, die als Kategorisierungsgrundlage bestehender Forschung dient und für die Erarbeitung einer Übersicht ebendieser herangezogen wird. Abschliessend werden wesentliche Einschränkungen, Trends und Herausforderungen des untersuchten Forschungsraums identifiziert.

Acknowledgments

Firstly, I would like to thank my supervisors, especially Jan von der Assen for their continuously inspiring and enthusiastic guidance. Thanks to Prof. Stiller and the Communication Systems Group for providing the organisational frame and offering the opportunity to work on this thesis.

Thank you to all the people who had to be particularly patient with me while my mind was dedicated to this project, instead of being present with them.

Contents

Chapter 1

Introduction

Cyberattacks have posed a threat to the success and continuity of businesses for a while already, however, a significant rise in incidents has been noted recently [1]. Cyberattacks are now considered one of the largest threats to business with investors finding that greater investments are therefore justified [3]. Another aspect which highlights the need for effective cybersecurity is that the cost of cybercrime to organisations is high and rising [1] - the Federal Bureau of Investigation (FBI) published the losses due to internet fraud to be 6.9 billion USD in 2021 [2].

With the rise of botnets, large numbers of devices that conduct cyberattacks cooperatively, the effectiveness of attack vectors has also increased [4]. Even more concerning is the fact that malware can now be bought from an online community, which provides the necessary support and assets to conduct cyberattacks [5]. Underlying these attacks are adversaries collaborating or cooperating with each other on various levels: technical, social, or economic. It seems therefore a natural consequence that to protect themselves against these sorts of attacks, defenders should also cooperate or collaborate with each other to detect vulnerabilities or mitigate attacks.

1.1 Description of Work

Firstly, the current state of cybersecurity is investigated. An overview of cybersecurity layers and threats is provided as well as trends dominating the field are discussed. Subsequently a number of frameworks which address cybersecurity are discussed.

Secondly, a schema is proposed by which existing literature can be organised. A definition of collaborative and cooperative cybersecurity is provided, and a taxonomy is proposed to appropriately categorise the selected literature. The taxonomy offers multiple perspectives, it is based on the NIST Framework [6], on a distinction between technical or non-technical approaches to cybersecurity, and on solution, function, and collaboration type.

Lastly, a survey of the literature is performed leveraging the proposed taxonomy. Following the review of the literature, fifty-four papers are categorised using the proposed taxonomy and then synthesized. Furthermore, key limitations, trends, and challenges of applying collaborative or cooperative approaches to cybersecurity are identified based on the literature. A discussion of open research questions concludes the thesis.

1.2 Thesis Outline

The remaining report is structured as follows. Chapter 2 provides an overview of the most relevant concepts in the field of cybersecurity and provides definitions for collaboration and cooperation. Chapter 3 discusses the related work including similar literature reviews proposing taxonomies, articles, and surveys. Consequently, the related works are discussed, and their most key features are highlighted. Chapter 4 describes the methodology used for this mapping study, among others, the research questions and search strategy are discussed. Chapter 5 describes the proposed taxonomy and summarises the findings. Chapter 6 discusses key challenges and opportunities to apply collaborative and cooperative settings and methods for cybersecurity. Finally, chapter 7 summarises the main contributions of the thesis and provides an outlook for future work.

Chapter 2

Background

Information technology has become central to the functioning of organizations, governments, and for the public [7]. The usage of electronics and information technology to automate production has been named the Third Industrial Revolution [8]. Societies, economies, and politics are increasingly more dependent on information and information systems - which are critical to energy, transport, communication, and healthcare [7]. It is therefore essential that the confidence in their reliability and well-functioning is preserved.

The goal of information security according to the International Organization for Standardization(ISO) [9] is to protect information by preserving its confidentiality, integrity, and availability (*cf.*, Subsection 2.1.2). Information security can be considered an old subject which came into existence long before the invention of computers - in the first century BC, Julius Caesar used secret codes to protect private information sent via messenger [10].

Returning to present times, ISO defines cybersecurity similarly, as the preservation of confidentiality, integrity, and availability in the cyberspace [11]. With the cyberspace being a complex environment that does not exist in physical form, but where people, software and services interact on the Internet through devices and networks [11]. It should be noted that the cyberspace is a dynamic, evolving system influenced by its growing numbers of contributors, and not a static system [12].

2.1 Cybersecurity

Cybersecurity is a topic of actuality in a world that becomes more digital and connected through the cyber-space. It has three main goals, confidentiality, integrity, and availability with a number of layers to protect these three goals from cyberattacks and malicious parties. Due to its importance number of frameworks that deal with cyberattacks have come into existence and will be discussed in this chapter.

2.1.1 What is Cybersecurity?

Cybersecurity is a topic of actuality in a world that becomes more digital and connected through the cyber-space. However, there are many variations in defining it - moreover everyone seems to have a different understanding of cybersecurity, making definitions highly subjective. [12] proposes the following definition:

> *"Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights"*

The definition aims to capture the diverse interactions between systems, humans and between humans and systems which are essential in cybersecurity. It shows that protection from any threats whether from intentional or unintentional sources and from natural disasters, whether predictable or unpredictable is necessary [12].

2.1.2 Goals of Cybersecurity

Six cybersecurity goals are mentioned in [13], the first three are focused on a balanced protection of confidentiality, integrity, and availability of data, also known as the CIA triad [14], [15] these are industry-wide recognised information security goals, the following three are often neglected but relevant and worth mentioning.

Firstly, *Confidentiality* relates to keeping information secret. Protected information should only be accessible to authorised parties and systems. Confidentiality in the cyber world is often assured with help of encryption - translation of data in an intelligible form for those without the right access [13], [16].

A second goal is *Integrity*, which refers to keeping the information correct and reliable. The validity of data against undesired changes should be ensured through its entire lifecycle - it should not be possible to modify data in an unauthorised way without detection. Closely related concepts are *consistency*, *accuracy* and *precision* of data and systems [13]–[16].

To complete the CIA triad, *Availability* relates to ensuring the accessibility of the data to authorised parties at any time and in whatever format desired. System availability also refers to the system continuing operations despite some misbehaving participants or when security breaches are underway. The prevention of denial-of-service attacks is necessary to ensure preservation of availability [13]–[16].

A further goal is *Accountability*, which is concerned with the validation of the information. It is the property of tracing every activity to the individual or process that performed it, without repudiation. Individuals shall not be able to deny sending a message or authorising an action, when in reality they did it. Non-repudiation means that parties involved in an activity cannot deny their actions. Finally, accountability also relates to system disclosure - at any time hardware, software, microcode etc. should be open for inspection [13]–[16].

Authentication relates to verifying an identity of a user, a device, or a process to allow access to systems [17]. The three most common factors used for authentication, are *(i)* something you know - a password; *(ii)* something you have - a smart card; and *(iii)* something you are - a biometric measure. Combining the three factors, provides for a strong individual validation method [13].

Finally, *Authorisation* deals with verifying the access to systems or resources. It also determines the correct level of access of a person after it has authenticated. The *principle of least privilege* states that a subject should be granted only the privileges it needs to complete its task, and nothing more. Authorisation beyond the needed one creates unnecessary vulnerabilities. Additionally, *Authorisation* also ensures the correct assignment of rights - for instance, whether a user can solely read or can edit a file [13], [18].

2.1.3 Cybersecurity Layers

The Defence in Depth (DiD) concept in cybersecurity refers to an approach whereby data and assets are protected by multiple layers of defence - including intentional redundancies which act as fallback in case a previous layer fails [13]. Also called the castle approach, in DiD there is no single point of failure. DiD measures are meant to provide time to detect and respond to attacks additionally to the main goal of preventing security breaches [19]. In [13] six potential layers of defence are described.

Social engineering attacks involve manipulating humans (*People*) into making security mistakes or revealing confidential information. The preference of humans for convenience and their trust to people they barely know leads to a critical challenge in cybersecurity - convenience vs. security [13].

The network can be seen as a boundary or a fence. Therefore, *Network Security* can be viewed as protection against outsiders accessing an internal set of systems and resources. Common protection methods are firewalls, intrusion detection systems, IPSs - combinations of firewalls and intrusion detection systems and security information and event management systems [13].

After penetrating through the People and Network layers, an attacker would have to deal with the *Computer System*, or host level - or the operating system (OS). The OS must deal with at least the following: separation, memory protection and access control [13].

Applications are a popular attack target as they are easier to exploit than an OS - this is the case because they require more updates. Moreover, applications have a lot more features than a standard OS - the ubiquitous Microsoft Word has over a hundred features. Therefore,*Application/Software Security* is an important layer. Tools designed to protect against application - based attacks mostly rely on knowing how an attack looks before it is performed, however, zero-day attacks target vulnerabilities which have not been noticed before [13].

Data is one the most valuable asset to an attacker. *Data Security* should ensure that data is protected in every state: at rest, in transit or in use. Protecting data at rest is the easiest and can be achieved by using asymmetric encryption - with key management being of utmost importance. Asymmetric encryption refers to a cryptographic system that is based on two pairs of distinct keys. Each pair contains one key known to others (the public key) and one pair known solely by its owner (the private key) [16]. In transit, data can also be protected through asymmetric encryption, however, for data to be protected in use, an additional feature needs to be added - the encryption must be asymmetric *and* homomorphic. Homomorphic Encryption allows users to carry out operations on data that is encrypted without having to decrypt it first, while achieving the same results, as if they were performed on the unencrypted data [13], [16].

Finally, the last layer is *Cloud Security*. The security is shared between the cloud customer and the provider based on their agreed service model. There are three primary service models available; based on infrastructure, platform or application [13].

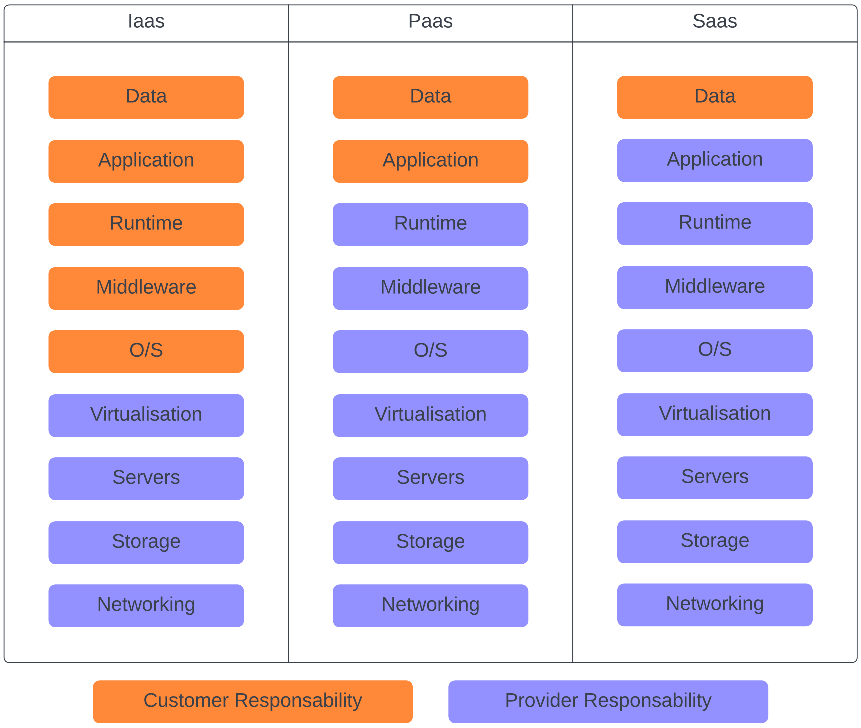


Figure 2.1: Cloud Service Models [13]

The foundation or first layer of cloud computing service models, is the *Infrastructure as a service (IaaS)*. It provides infrastructure for large, enterprise customers who need unlimited storage and computing power without having any hardware on site [20]. IaaS includes components such as virtual server space, network connections, bandwidth etc, which organisations can access to build their own IT platforms. Therefore, it enables clients to expand or modernise their IT competence without the need to allocate large financial resources to infrastructure projects. Scalability, location independence, no single point of entry, and the physical security of data centre locations are advantages that the IaaS model provides. However, the infrastructure of the cloud consists of multiple connecting data centres through local area networks across different geographical regions introducing vulnerabilites related to the internet, distributed denial-of-service (DDoS), Man-in-the-middle attacks (MITM), port scanning and IP spoofing. Finally, network monitoring is more challenging than in traditional network systems [21].

Platform as a Service (PaaS) provides a platform including a number of resources - operating system (OS), programming language, database and web server that scales to meet the demands of the application [20]. Traditionally companies must invest a lot of time and work to build a platform to run the software applications and to subsequently provide continuous administration. This model is often used by software companies to host and develop applications. They can loan a set of toolkits to develop a platform for deploying their applications. Advantages of the PaaS model include storage and server overhead, software maintenance, network bandwidth and support personnel. However, security issues arise from its design as a service-oriented architecture, and these include MITM; Denial-of-Service (DoS) and injection attacks [21].

Finally, in *Software as a service (SaaS)* all users share a common infrastructure. The software and data are hosted and deployed on the internet and are accessed by the customer through a web browser, meaning that he does not have access to underlying architecture such as servers, storage or operating systems [20]. Users do not have to concern themselves with the installation, maintenance, or software updates. Advantages to this model include patch management, easier administration and collaboration, global accessibility, and compatibility. However, application, process and network logs also sit with the vendors on virtual machines, which might lose files after power off - this robs security experts of the opportunity to analyse the log information and investigate malicious attacks. Finally, as SaaS builds on the IaaS and Paas models the challenges of the latter are also inherited by the former [21].

Figure 2.1 provides an overview of the three types of service models discussed and highlights which areas are within the responsibility of the client and which are within that of the provider. As discussed, the IaaS model shows the most customer responsibility, while in the SaaS model most of the responsibility is shifted to the provider, leaving only data to be secured by the client.

2.1.4 Cyberattacks

Determining how an attack was performed, the location and identity of the attacker or of an attacker's intermediary is the process of attribution of an attack, and often poses a challenge [22]. It includes an investigation into all aspects of the attack with the aim to answer the questions: who, why, what, where and how the attack happened [13]. To simplify this process, three main concepts are used.

Potential events that might impact an impact a network or an information system are *threats*. They are often confused with types of attacks. [13] explains how ransomware a word many outside of the cybersecurity field associate with a threat in fact an attack - the threat is the availability of the hard drive or files that might be compromised. Table

Table 2.1: Cyber Threats [13]

Goal	Definition	Threat
Confidentiality	Keeping information secret	Information will not be kept secret
Integrity	Keeping information correct and reliable	Information cannot be trusted
Availability	Ensuring information is available to the right people at all times	Information will not be available
Accountability	Validation the source of an action	The source of action cannot be verified
Authentication	Verifying an identity	Identity cannot be verified
Authorisation	Verifying access to resources	Access to resources cannot be verified

2.1 shows the relationship between the cybersecurity goals (*cf.*, Subsection 2.1.2) and the threats they might face.

Vulnerabilities represent potential threats resulting from an error or weakness in the system [13]. Sponsored by the U.S. Department of Homeland Security, the Common Vulnerabilities and Exposures(CVE) list provides an overview of all publicly disclosed vulnerabilities [23]. Furthermore, the U.S. Department of Commerce keeps a list of all CVEs it receives as well, and for reference just this week[1], close to 600 events were received [24].

Bringing the threat and vulnerability concepts together, is *risk*, described as the probability that a threat actor will exploit a vulnerability, while taking into consideration how severe the impact of this would be [13]. The relationship described can be summarised in the following formula:

$$risk = threat \cdot vulnerability$$

The impact is a qualitative assessment of the effect to the asset in question. There is a significant difference between an attack which takes down the website of a large e-commerce business such as Amazon, or the website of a small hotel in Greece. Amazon produces large revenues in an hour whereas the hotel might not lose many bookings over one hour. The risk has therefore a subjective aspect based on the security expert's bias towards certain types of vulnerabilities and threats, and the perceived impact of an attack [13].

The Open Web Application Security Project (OWASP), an online community publishing information on web application security, releases a Top Ten web application security risks. Their 2021 Top Ten are enumerated and explained in Table 2.2 [25]:

Similarly, the European Union Agency for Cybersecurity (ENISA) publishes an annual report [29] on the status of the cyber threat landscape as well as the most important threats identified during the year. The prime threats identified in the latest report which covers the time between April 2020 and July 2021 are discussed below.

[1] Week starting 8th of August 2022

Table 2.2: OWASP Top Ten Web Application Security Risks [25]–[28]

Risk	**Sample attack result**
`Broken Access Control`	Misconfigured permissions allow attackers to access information that they should not have access to, leading to unauthorised data disclosure, modification, or destruction
`Cryptographic Failures`	Sensitive data is insufficiently protected, leading to disclosure of passwords, credit card numbers, or other private information
`Injection`	Inserting malicious code into a program which aims to execute unintended actions to gain access to sensitive data
`Insecure Design`	Distinct from insecure implementation, it refers to architectural flaws - a secure implementation with insecure design still translates to a vulnerable web application
`Security Misconfiguration`	Broad range of potential vulnerabilities including incomplete configurations, enablement of unnecessary features, default accounts and related passwords still enabled
`Vulnerable and Outdated Components`	Developers are unaware of the versions of components including for nested dependencies or of the fact that the software is out of date, unsupported or vulnerable
`Identification and Authentication Failures`	Incorrectly implemented authentication leading to attackers assuming legitimate users' identities
`Software and Data Integrity Failures`	Failure to verify the integrity of software patches and updates before implementation on servers and applications
`Security Logging and Monitoring Failures`	Poor monitoring practices and failure to log errors leading to slower incident responses emphasizing potential damages of breaches
`Server-Side Request Forgery`	Web application fetches data without validating user-supplied URL leading to data exposure, DoS attacks or Remote Code Execution

Ransomware is an attack where assets, usually data of an organisation are encrypted and the attackers demand payment to restore access to the information. As the incidence of such attacks has increased, a series of policy initiatives related to the topic have been proposed both in the European Union (EU) and worldwide [29].

Software aimed at performing malicious processes that have an adverse impact on the CIA goals of cybersecurity (*cf.*, Subsection 2.1.2) constitutes *Malware.* A positive development is that malware attacks have decreased recently [29].

Cryptojacking is a more recent threat which is related to the proliferation of cryptocurrencies. Cryptojacking refers to the process whereby an attacker used the victim's computing power to mine cryptocurrencies. With the increase of public interest in cryptocurrencies this type of attack has increased lately [29].

People are often the first target of attackers (*cf.*, Subsection 2.1.3) and *E-mail related attacks* refer to a number of threats where attackers exploit vulnerabilities of humans rather than system vulnerabilities - these include spam, phishing malware such as spyware and Trojan horses. Despite numerous awareness campaigns and education initiatives against these attacks the threat persists and even increases - especially in the case on attacks on business e-mails with the aim to extract monetary gains [29].

Releasing of confidential or sensitive information to a malicious player are referred to as *Attacks against data.* Access to data is a target for attackers because of numerous reasons, for instance, sensitive data can be used for extortion, misinformation, ransom requests, and many more [29].

Numerous attacks target *Availability and Integrity* with the major ones being Denial of Service (DoS) attacks and Web Attacks. The former threatens IT systems, and targets their availability by exhausting resources, leading to decreased performance, service outages and loss of data [29].

Disinformation - Misinformation campaigns are increasing, due to the increased usage of social media and online media platforms, as well as the increased amounts of time spend online because of the COVID-19 pandemic. A fairly new threat, campaigns of disinformation and misinformation frequently are used in hybrid attacks to decrease the trust of people [29].

Often based on human errors or misconfigurations of the systems, *Non-malicious threats* can be regarded as accidents. Natural disaster that negatively impact IT infrastructure can also be included in this category. Inevitably these threats can never be reduced to zero and hence constantly feature on threats lists [29].

Figure 2.2 gives an overview of how the three items above, threats, vulnerabilities and risks relate to other cybersecurity concepts. For example, starting from the threat agent, this originated a threat, to exploit a vulnerability which leads to a risk that an asset can be damaged. A multitude of similar deductions can be made, and this emphasizes the point how interconnected all the factors presented above are.

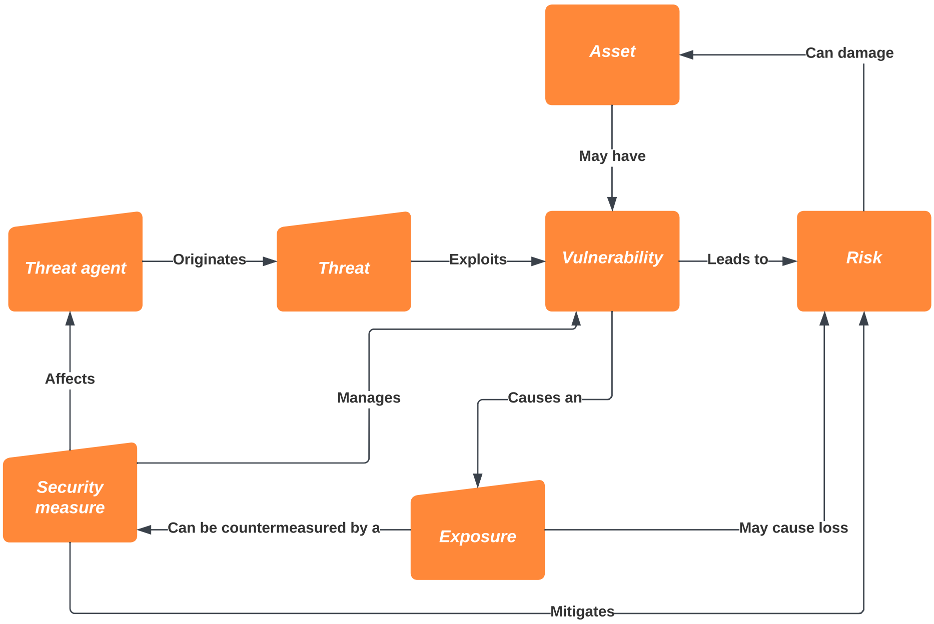


Figure 2.2: Security measures relationships with other concepts [7]

2.1.5 Cyber Kill Chain

Identifying threats, vulnerabilities and assessing risk constitutes a cyber risk assessment [13] - this is a comprehensive way to investigate how attackers can exploit targets. The process of exploiting targets is introduced in a cyber kill chain model. The Cyber Kill Chain (CKC) was developed by the Lockheed Martin Corporation - aiming to deal specifically with Advanced Persistent Threats (APTs), attackers which are relatively advanced and more persistent in their approach [30]. The CKC identifies seven steps which attackers need to complete to achieve their objective [13], *i.e.*, to perform a successful attack. Figure 2.3 highlights the 7 steps and their order.

Reconnaissance refers to researching and gaining information about a target and find potential weak points that can be exploited, as well as identifying and finally selecting the targets [13], [30]. The next step, *Weaponization* involves creating an exploit, based on the weakness discovered during the previous stage. This is coupled with a trojan, for example, into a deliverable payload - MS Office documents or PDFs can serve as weaponised deliverables [13], [30]. The *Delivery* involves delivering the payload to the targeted network or device. Popular ways are through email, malicious websites, or USB sticks and other removable media [13], [30].

After the payload is successfully delivered, the *Exploitation* step refers to the running of the application to exploit the weakness identified [13]. *Installation* is closely related to the previous step - if the exploit was successful, the malicious code is installed in the victim system for the attacker to keep their presence in the system even in case the system is rebooted [13], [30]. *Command and Control* refers to the fact that the exploit will have

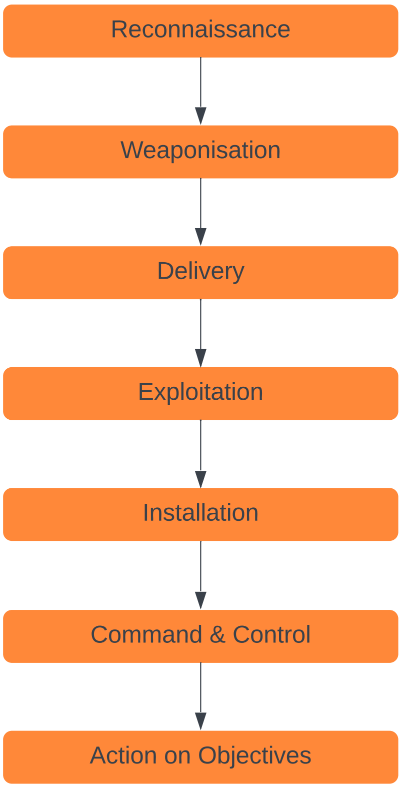


Figure 2.3: The stages of the Cyber Kill Chain [30]

the ability to correspond with the attacker from the victim system - the channel for the attacker to have remote access to the compromised system is established [13], [30].

Finally, *Actions and Objectives* refers to the step where the act of executing the objective against the target - DoD attacks, data theft, compromising additional systems, moving laterally inside the network, etc. [13], [30] is completed.

2.1.6 National Institute of Standards and Technology Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a U.S. government-ordered framework aiming to provide a guideline for mitigating risks and better protect physical assets as well as information from cyberattacks. Its adaptability makes it in essence an industry standard, as it can be adapted to a large number of operating environments [19]. The NIST Framework is comprised of 5 core functions discussed below based on [6].

Firstly, *Identify* refers to understanding how to manage cybersecurity risks to data, systems, assets, and capabilities - in essence you need to know what to protect, to be able to protect it [19]. *Protect* relates to safeguards needing to be implemented to ensure the delivery of critical infrastructure services. *Detect* means that checks need to be developed and implemented to identify cybersecurity events. *Respond* activities need to be developed and implemented to action on detected cybersecurity events. And finally, *Recover* activities must be developed and implemented for resilience and to restore any services or capabilities that were impaired dur to cybersecurity events.

Each function is further divided in a number of categories, and categories in subcategories. A more detailed discussion of the former will be provided in the Findings (*cf.*, Chapter 5).

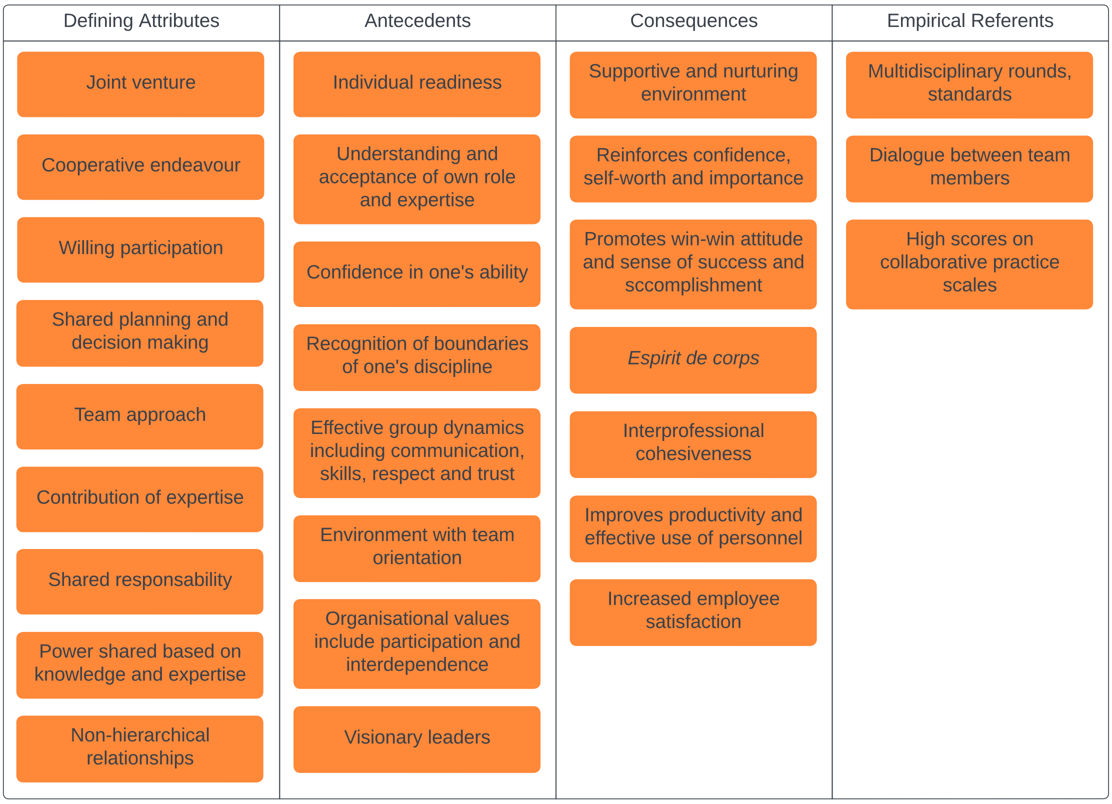
2.2 Collaboration and Cooperation

The second main concept that is relevant to this thesis is the paradigm of collaboration and cooperation. The emergence of collaborative cyberattacks, and the interconnectivity of the times [31], [32], pose the question of whether cybersecurity could also benefit from a collaborative approach to protecting from attacks [33]. The concept of collaboration is ubiquitous today, however, not much thought is dedicated to understanding it. This section aims to provide some clarity around the concept.

2.2.1 Fundamentals of Collaboration and Cooperation

Collaboration can be described as a process which stresses a joint involvement of multiple parties in intellectual activities [34]; a cooperative endeavour based on shared authority and power; non-hierarchical in nature - assuming power based on expertise and knowledge, rather than on function or role. For collaboration to work, it is required that individuals see themselves as being part of a team, while contributing to a shared goal where all parties offer their expertise and share responsibility for the result [34]. Figure 2.4 provides a summary of defining attributes, antecedents, consequences, and empirical referents related to collaboration. Interestingly the author includes ”cooperative” endeavours as an attribute of collaboration, and while the contrast between the two is discussed in more detail below, it could be interpreted here that cooperation is a less strong form of collaboration, missing some of its features.

Collaboration and cooperation, also come with hurdles. One essential one is the conflicting need of anonymity versus trust [33] - collaborators need to protect their source of information, or stay anonymous themselves, but also to validate the information that other contributors share. Comparing this relationship with similar communities [33], found that cyber-security information sharing can be well likened to open-source software projects with 3 motivators for participation being:*(i) Paying it forward* - Sharing information might help peers, which in turn will hopefully share with me in the future. *(ii)Peer reputation* - Acknowledgment from peers is important, and being the first to find, understand and deal with an issue is something to be shown. *(iii)Common cause* - Working together with those in the same geographical area, industry, etc. to protect against a common threat [33].



Defining Attributes	Antecedents	Consequences	Empirical Referents
Joint venture	Individual readiness	Supportive and nurturing environment	Multidisciplinary rounds, standards
Cooperative endeavour	Understanding and acceptance of own role and expertise	Reinforces confidence, self-worth and importance	Dialogue between team members
Willing participation	Confidence in one's ability	Promotes win-win attitude and sense of success and sccomplishment	High scores on collaborative practice scales
Shared planning and decision making	Recognition of boundaries of one's discipline	*Espirit de corps*	
Team approach	Effective group dynamics including communication, skills, respect and trust	Interprofessional cohesiveness	
Contribution of expertise	Environment with team orientation	Improves productivity and effective use of personnel	
Shared responsability	Organisational values include participation and interdependence	Increased employee satisfaction	
Power shared based on knowledge and expertise	Visionary leaders		
Non-hierarchical relationships			

Figure 2.4: Key Dimensions of Collaboration [34]

In the case of open-source projects, as participants share information, this can be assessed through open peer review. Sharing of correct information consistently over time builds the reputation for the owner of the account which shares information - creating a positive feedback loop. However, if contributors choose to stay completely anonymous, the inability to tie contributions to an account, will hinder the ability of building a reputation, and hence verify the originator of information [33].

Collaboration also implies a higher time demand for parties [35] - there will always be a time where communication is necessary among collaborators; whether during regular meetings, or for an ad-hoc discussion, parties will have to align themselves somehow, and this will require time. For international teams, which are working across time-zones, it is particularly difficult to find a suited time to fit everyone - take the US East Coast and Japan, they have no overlap over traditional working hours [36]. Additional challenges for international teams can be language barriers, which can hinder communication and lead to misunderstandings, or procedures and work habits varying from nation to nation [36]. Across cross-disciplinary teams there can arise issues with the perceived value of collaboration across different professions, moreover, inadequate understanding about different disciplines might induce value conflicts among collaborators from different disciplines. Each will think that their area is the most important and will disregard others. Additionally, technical hurdles to collaboration can also exist. In the context of cybersecurity, for example, collaboration with domain experts who have little to no knowledge about security methods might be necessary [37]. Finally, each person has a unique attitude and style of working, some potentially not conductive to teamwork at all, possibly creating tensions and difficulties in collaboration [35].

More broadly, collaboration between multi-organisation groups have the following characteristics: *(i) No authority hierarchies*, by definition, there are no formal power hierarchies within a multi-organizational therefore, a typical incentive for participation - requirement to do so - is missing. This means that participants need to have some intrinsic motivation to participate and to believe in the value of collaboration. *(ii) No history*, often collaboration will occur between people who have no experience working together, and potentially will only work on one project together. This can be an advantage, as the collaboration will start as a blank slate rather than with unhelpful ingrained practices, however, issues can arise when a decision must be made between developing a set of working ”rules” or accepting that work will continue without properly defined ones. The first option might be regarded as a waste of time by some participants, while the second one seems likely to increase confusion or inconclusion.

Another aspect of collaboration to consider when aiming to improve a tool, method or process is that it can take many forms. *Teams and collaboration* - the aim of this type of collaboration is to build teams where team members need to communicate, collaborate, and complete tasks irrespective of time and space. Usually led by a team leader to keep the equilibrium , work and speed might however be affected by concepts such as task value, perceived task interest, individual attitude [38], [39]. A collaboration between an expert and a novice, with the former guiding the latter is referred to as *Mentorship and coaching* [38].

Similarly, to team collaboration, *Peer-to-peer feedback* involves people interacting with each other, but unlike in a team, communication, knowledge, and feedback sharing is not within the entirety of the team, but a one-to-one basis between the members [38]. *Debate and discussions* refers to collaboration in small groups based on critical discussions. This type of collaboration facilitates the process of learning by representing, constructing, and sharing of opinions with the aim of learning [38]. *Social collaboration* is a form of collaboration where individuals can reach out to others quickly to discuss issues and try finding solutions [39].

Teams from different departments (in organisations) or verticals work together *Cross-functionally* to accomplish a common goal [37], [39]. *Community collaboration* is closely related to team collaboration, this type of collaboration encourages a sense of community within a team. As opposed to the typical teamwork focused on performing tasks or completing work, importance is placed on learning and sharing knowledge within the team while removing strict hierarchies [39].

2.2.2 Distinction between Collaboration and Cooperation

Collaboration and cooperation are two related concepts which are often used interchangeably [40]. Their similarities include but are not limited to the fact that both involve teamwork of some form, within entities or regions, or across countries and industries for varying lengths of time [40]. However, differences do exist between them, and researchers do distinguish between them [41].

In general, cooperation involves some independent work of the member of the cooperating group, with members taking responsibility for particular sub-tasks [41], [42]. Typical characteristics of cooperative tasks are division of labour, task specialisation and individual responsibility for the final product [42]. Members agree to share information with each other and support each other, without them working together towards the final goal - the relationships are therefore usually external and horizontal [40].

Collaboration, however, does not include task specialisation and all group members must work synchronous on a number of aspects of a project [41], [42]. Collaborative relationships involve direct participation of parties in designing producing a final product, with the relationships being vertical [40]. Some argue that collaboration could improve the quality of the end result, while cooperation would provide for faster, more convenient task completion [41].

Combining the information presented in this chapter and looking specifically at the field of cybersecurity, cooperation, and collaboration we propose the following definitions of cooperative and collaborative cybersecurity.

Definition 1.1 *Cooperative Cybersecurity* The organisation and collection of structures, processes and resources which include at least some aspect where collective effort is used and it is divided across multiple actors, used to protect the cyberspace and cyberspace-enabled systems from incidents that misalign de jure from the facto property rights.

Definition 1.2 *Collaborative Cybersecurity* The organisation and collection of structures, processes and resources which include at least some aspect where collective effort is used and multiple actors work synchronously to achieve it, used to protect the cyberspace and cyberspace-enabled systems from incidents that misalign de jure from the facto property rights.

The definitions are based on a cybersecurity definition proposed in [12], and as discussed capture the diverse interactions between systems, humans and between humans and systems which are essential in cybersecurity. They show that protection from any threats whether from intentional or unintentional sources and from natural disasters, whether predictable or unpredictable is necessary. Additionally, the cooperative and cooperative aspects must allow for the interpretation to refer to both interactions between multiple machines, multiple humans, or machine-human interactions, while capturing the discussed contrast between the two.

Chapter 3

Related Work

As discussed in the definition of the search process (*cf.*, Subsection 4.2), a search of cybersecurity and cooperation or collaboration yields a large amount a results. Of high importance nowadays, a lot of research has been devoted to the topic. Because of the increasing amount literature and the fact that cooperation and collaboration can be applied to cybersecurity in a multitude of ways, it is of interest to find a way to classify the literature and make sense of the interactions between cybersecurity, collaboration and classification.

Despite this, little scientific work proposing a taxonomy of cooperation and collaboration in the context of cybersecurity was identified. A large number of different literature reviews or mapping studies are available covering the topics of cybersecurity, and collaboration or cooperation individually and some relevant ones are covered in this chapter. Before discussing works that are related to the topic at hand in more detail, it is important to discuss three different types of papers which are distinguished in this chapter.

Literature review, also referred to as literature survey and mapping study, refers to work that investigates topics by going through available literature. This is done to identify the research directions available for a broader topic, as well as to identify novel directions that could be considered. These reviews can also incorporate, but do not always do, a taxonomy or categorisation of sorts to provide a more accessible overview of the topic.

In this chapter, *Survey* refers to a process whereby a list of questions is directed to a relevant population sample in order to get an insight into their field. The work then looks at answers provided and tries to identify similarities and trends.

Articles simply refer to any research work. This does not usually involve synthesizing information from other research sources on a broader topic, but refer strictly to one topic which might be investigated in more detail.

One of the goals of this thesis is to propose a definition of collaboration and cooperation that is appropriate to the field of cybersecurity and to propose key dimensions by which approaches that fit the definition can be categorized. Given the lack of literature reviews with the exact same direction as the present work *i.e.*, the proposal of a taxonomy which can be used to appropriately categorise works investigating cybersecurity and cooperation and collaboration and a survey of all artifacts identified from academic sources selected after the search process, the related work serves to present works that are similar from different points of view.

As such, the works below are inspected from the following perspectives: *(i) Topic or Contribution* the focus here was on works investigating cooperation, collaboration or cybersecurity. The *(ii) Methodology* is an important aspect of mapping studies. Therefore, related work was investigated to find out what state-of-the art approaches to search protocols exist. *(iii) Results* were investigated focusing in particular on taxonomies that were proposed. This is to get an understanding of what kinds of taxonomies existing in the discussed fields, as one of the main goals of this work is to provide a taxonomy to appropriately categorise works investigating cybersecurity and cooperation or collaboration. Finally, *(iv) Future Work* proposals were considered, especially whether research directions that could be interesting and useful to investigate further based on the information discovered in the respective study were identified. All these properties are essential parts of this work as well, and it is reasonable to use them to contrast related work and gain an understanding of what already exists and what is missing from the literature.

[43] proposes a literature review which focuses on various collaboration mechanisms and defence in collaborative security. The most closely related identified work to the topic of this thesis, the study discussed the scope of collaborative security, and identifies the components which are essential for it. Multiple mechanisms of collaborative security are analysed and finally challenges that can arise during the design of collaborative security are discussed. The paper does not specify the methodology used.

The proposed taxonomy includes seven principles: analysis target, network infrastructure, interoperability, timeliness, architecture, shared information and initiative. 44 systems are analysed based on the proposed taxonomy. Finally, five challenges in designing collaborative security systems are identified - privacy, scalability, accuracy, incentive and robustness. Coupled with the coverage of collaborative security trends, the challenges provide a blueprint on which future research on the topic can be based.

In [44] it is argued that given the technologized times that we are living through now, network-based systems are faced with an ever-growing array of cyber-attacks on a daily basis. Traditional cybersecurity methods rely on threat-based databases which have to be updated daily in order to bring them up to speed with the new cyber-threats so that they can continue protecting the underlying network-based systems. Additionally, sensitive data generated by applications must be managed and processed. In recent years, a number of computing platforms based on representation learning algorithms have been developed. These are a resource to exploit as well as manage the generated data and extract useful information from it. The survey conducted by the authors highlights various real-life examples of cyber-threats and initiatives adopted by organisations to deal with these threats. This work does not specify the methodology used.

[44] does not propose a novel taxonomy, but it provides an in-depth overview of cyber-attacks, initiatives taken by international organisations to combat them; as well as an overview of various representation learning techniques, computing platforms and datasets suitable for use for representation learning in the cybersecurity domain. Limitations and

future work are discussed extensively, and future research directions are proposed for each one of the discussed topics.

In [45] changes that are happening during our times thanks to increasing internet connectivity are highlighted. Cloud technology and the development of Internet of Things (IoT) lead to an increase in interest in decentralised methods for trust management. The contributions of this literature review are

- A systematic review of 272 papers and 128 business initiatives related to cybersecurity in the context of blockchain
- A taxonomy of cybersecurity properties, related techniques, fields where these are relevant, technologies and justification for using blockchain
- An overview of lessons learned and recommendations for future research

The methodology is well described and uses a number of steps to ensure validity and repeatability of the survey. The steps are, identification of the research questions, search and selection of relevant work, extraction of information, synthetisation and reporting. The sample of relevant work was 272 articles. The taxonomy provided is extensive, as it classified the academic papers based on three cybersecurity properties: authentication, non-repudiation and confidentiality. Interestingly these belong to the goals of cybersecurity discussed previously (*cf.*, Subsection 2.1.2), however only one of these is usually considered as the main goals and included in the CIA triad. Further classifications were made based on cybersecurity techniques, technology and area. Finally, the authors classify the literature on whether the use of blockchain is justified.

The lessons learned by the authors in [45] are that academic interest in the topic of blockchain and cybersecurity has started increasing immensely since 2016. It seems that Ethereum is the preferred technology for both the academia and the industry, with the former mostly justifying the use of the blockchain technology. Industrial proposals often omit key details in their approaches and even more worrisome is that some academic papers are using blockchain without adhering to the principles justifying its use.

[46] presents a systematic literature review to investigate the topic of Industrial Internet of Things (IIoT). Four areas were analysed in this paper:

- Definitions of the topics of information security awareness and cybersecurity awareness
- The industries of the papers surveyed, in order to understand where there are gaps
- What techniques companies are using to increase cybersecurity awareness
- Benefits of raising awareness across organisations

The methodology used by the authors is based on the systematic literature review approach. And was divided in four main stages: planning, search execution, document analysis and result reporting. Each with a number of sub tasks. The selection of resources for the review resulted in 23 scientific papers which were analysed. The results were well presented in a final tabular outline. A taxonomy of sorts was created for each of the four items enumerated above.

Cybersecurity and information were *defined*, with similarities and contrasts being discussed. A number of *target industries* were discovered - cybersecurity awareness in the context of manufacturing, critical infrastructure and generally with reference to IIoT environments. But the review also highlights the need for more targeted studies in the area of cybersecurity awareness. Commonly used *models and tools for raising cybersecurity awareness* were discussed and contrasted. And finally, *benefits* were highlighted. Interestingly, although not identical, these had some overlap with the NIST framework. The main elements proposed by the authors in this case are: *(i)* Identify, *(ii)* Reduce, *(iii)* Prevent, *(iv)* Improve and *(v)* Protect.

The authors find that despite the relevance of the topic of cybersecurity awareness in the industrial context based on the IIoT paradigm, literature investigations are not prevalent. No specific future work topics are defined; however, a general direction is proposed by the authors, in more focused cybersecurity awareness studies for the fields of manufacturing and critical infrastructure.

Based on the belief that the rush to develop applications for smart cities leads to a lack of appropriate implementation of security and privacy for the applications, [47] investigate practical and theoretical opportunities and challenges in the system deployments in smart cities. The study investigates the following:

- Analyse the latest developments in the field of cyberattacks on smart cities
- Investigate well-known attacks that were deployed against smart cities infrastructure
- Provide technical solutions that aim to mitigate the vulnerabilities of the smart cities against different attacks

The methodology is not specifically mentioned by the authors. The paper seems to go through a large number of papers in order to provide an overview of the literature. No taxonomy is provided. As a conclusion, the authors encourage a holistic approach to the implementation of secure smart cities. Where technological work to improve the hardware and software components of the smart cities, is simultaneous with joint efforts of all stakeholders (citizens, governments, policymakers etc.) to address the challenges of the field. Although not mentioned specifically, smart cities are inherently collaborative, an aspect discussed later in this report (*cf.*, Chapter 5).

[48] looks at cybersecurity in the context of construction - an area that has borrowed general solutions and frameworks, as its phases have become increasingly digitalised while making use of information and communications technologies. The goals of the paper were two-fold. Firstly, to provide a framework to study cybersecurity in construction in particular and secondly, to identify the main cybersecurity threats based on the framework

The methodology is extensively discussed. It involved analysing various general cybersecurity frameworks and standards as well as first principles of systems theory and process engineering, and research literature.

This work first discusses existing cybersecurity frameworks such as NIST [6], NIS, the IET code of practice. The aim of the authors is to investigate how each framework decomposes the cybersecurity world in parts, what vulnerabilities each of the parts could have and the processes that could make them more secure. Consequently, it proposes a novel framework based on three concepts: confidentiality, integrity and utility - a classification similar to the CIA framework discussed in (*cf.*, Subsection 2.1.2). Each one of the above concepts are applied to four relevant categories in the construction world: physical objects, information, people and systems.

Finally, the authors regard their work as a standalone tool to distinguish challenges in cybersecurity and as an aid to structure future research. No future work is specified, other than the fact that the proposed framework shall serve as a tool for construction professionals to develop checklists and templates to improve cybersecurity

[49] argues that the increased volume of data, speed and diversity of cybersecurity attacks employed nowadays, pose challenges for signature-based cybersecurity strategies. Consequently, it investigates various artificial intelligence (AI) based solutions for cybersecurity. The paper aims to answer the following questions.

- Which cybersecurity techniques are significant to cybersecurity?
- How can cybersecurity stakeholders apply deep learning to various cybersecurity problems?
- What data sets are available for training, validating and testing deep-learning based cyber-defence systems?
- What successful deep learning based cybersecurity systems have been developed lately?
- What are relevant areas in which further study is warranted?

The methodology involved finding current types of cyberthreats and matching them against the threat report from ENISA. Subsequently relevant literature for the selected threats was investigated. The number of analysed research works was 75, spanning from 2016 to 2021. The number of works investigated increased with the year, ensuring that more recent work was well represented.

The results of [49] involved the proposal of a framework, deep learning framework for cybersecurity applications (DLF-CA) which included the following steps: (1) Problem formulation, (2) Collecting data, (3) Pre-processing the data, (4) Problem formulation, (5) Feature extraction, (6) Model selection, (7) Training and validation, (8) Evaluation. The framework seems to be based on the most common steps used for machine learning (ML) projects. These are common in a number of different fields where ML is used [50]–

[52] as well as in the industry [53]. The paper then continues with a survey of the literature. A large number of suggestions for future investigation potential is identified.

Deception is commonly used in cybersecurity for attacks, [54] investigates deception from a defence perspective. The contributions of the paper are the following:

- A review of game-theoretic models used in connection to privacy and cybersecurity
- A survey of contributions in the field of game-theoretic defensive deception
- A taxonomy based on the contributions discussed - this distinguishes various types of deception in order to enable a classification in terms of game-theory
- Areas of future research

The survey of the literature is based on 24 articles published between 2008 and 2018 in the fields of cybersecurity or privacy that employ defensive deception and use game theory.

[54] main contribution is the classification of deception into six types: perturbation, obfuscation, mixing, moving target defence, honey-x and attacker engagement and to define them. Additionally, it provides a snapshot of the literature at the time of the research. Areas of future work are identified, these include theoretical advances where other game-theoretic models are used; practical implementations; and interdisciplinary security - recognising that in the fields of economics, psychology and criminology there is valuable research that can be used.

The following literature review [55] investigates moving target defence (MTD) in the context of Internet-of-Things (IoT) systems. Specifically, the authors identify and synthesize MTD techniques for IoT and examine whether MTD is a fitting cybersecurity approach for IoT systems. The contributions of the review are threefold:

- A review of MTD techniques for IoT systems.
- An assessment of the techniques identified in terms of their security status and the feasibility of using MTD techniques for the IoT.
- Four new entropy-related metrics and their practical application.

The methodology is described extensively and is based on the systematic literature review by [56]. The review follows the main three steps of planning, conducting and documenting. The search of relevant material is done using the main research databases - IEEE Xplore, ACM Digital Library, Springer Link, Wiley Online Library, ScienceDirect and Scopus. Finally, the entire process is highlighted in multiple schemes which makes the methodology clear.

The review does not propose a novel taxonomy but uses standard MTD taxonomies to categorise the MTD techniques. The authors find that MTD is feasible for IoT and has real-world deployability. Finally, the work identifies future research opportunities.

Table 3.1: Overview of related work

Paper	Main Topic	Methodology	Related Work	Taxonomy	Future Research
[43]	Collab. and Cy./Security	✗	✓	✓	✓
[44]	Cy./Representation learning	✗	✗	✓	✓
[45]	Cy./Blockchain	✓	✓	✓	✓
[47]	Cy./Smart cities	✗	✓	✗	✓
[48]	Cy./Construction	✗	✓	✓	✗
[49]	Cy./Deep learning	✓	✓	✓	✓
[54]	Cy./Defense	✓	✓	✓	✓
[55]	Cy./Defense	✓	✓	✓	✓
[58]	Collab./Networked organisations	✓	✗	✓	✓
[59]	Collab./Software development	✗	✓	✓	✓

Cy. = Cybersecurity, Collab. = Collaboration, Coop. = Cooperation

As opposed to the literature surveys discussed above, [57] is a survey where participants are asked to answer a number of questions in order to draw meaningful conclusions. This survey is particularly relevant, because it investigates the attitude of companies - both software providers, and software acquirers or users - towards sharing vulnerability information. The sample size is rather small, and it consists of only 17 Swedish companies, however the results are worth noting. The authors show that although having a positive attitude towards sharing vulnerabilities within the software ecosystem, companies don't share proactively or in a planned fashion. This leads to the conclusion that the perception of the desired position is not aligned with the reality for the companies surveyed. Furthermore, companies seem to consider the sharing of vulnerability information to be sensitive. Government agencies are recommending proactive vulnerability disclosure based on the idea that cybersecurity will be improved if all actors in a software ecosystem cooperate.

Finally [60] investigates collaboration and the NIST framework to increase campus collaboration on IoT (Internet of Things) projects at West Texas A&M University. The university has adopted the NIST framework, which is widely used across organisations - by 30 percent of organisations in 2016 and projected to reach 50 percent until 2020 [61]. The usage of the framework for cybersecurity and the collaboration between multiple stakeholders lead to the development of several IoT initiatives such as smart-connected parking, and water irrigation management techniques to optimise water usage. The paper shows the importance of using an intuitive and easily comprehensible framework to develop and raise awareness of cybersecurity, in the context of a notoriously fragmentated environment where system administrators located in different each department and IoT efforts launched by non-IT personnel.

In [58], the authors perform a literature review on the topic of business models for collaborative networked organisations (CNO). A taxonomy of business models is presented and subsequently the information is used to discuss potential design for management and governance models for cybersecurity competence networks. Sixty various sources of academic literature were reviews to reach their conclusions. These incudes books, journal articles, conference papers etc.

A taxonomy is provided and highlights different types and degrees of collaboration. For example, based on the goal and horizon of collaboration, there is a long-term strategic type of collaboration and a goal-oriented, opportunistic type. The paper also highlights two interesting concepts related to collaboration that can be applied to future cybersecurity collaboration projects.

Virtual Organisations Breeding Environment involve establishing a long-term alliance of parties to increase the preparedness for concrete cybersecurity collaboration projects, by first setting up a cooperation agreement and building relationships at organisational and personal levels. While *Virtual Organisation* are a geographically dispersed and temporary network of entities that work together around a particular shared goal at some point in time. The team of authors identify a further research topic which will be investigated by themselves.

In [59] the authors develop a framework emphasizing the collaboration needs of developers. Based on Maslow's hierarchy of needs, the proposed framework also classifies the needs into *basic*, *enhanced* and *comfort* needs. The paper does not specify the methodology used.

Figure 3.1 presents the proposed collaboration needs hierarchy. Apart from the three broad classes of needs, the pyramid also consists of three basic strands, namely communication, artifact and task management. The base layer of the pyramid represents the basic needs, such as communication and task distribution. The two levels show the enhanced needs, conflict resolution, parallel development access rights etc. Finally, the top two layers represent the comfort needs and include context aware applications and continuous coordination, among others. One final aspect to note is that the distinction between the three strands gets blurred with each higher level. This is based on studies showing that users might combine various resources and cues to coordinate. For instance, artifacts can become communications medium, bug reports, or be used for task management, requirement specifications.

The authors use the framework to classify the Eclipse plugins. The need to perform further research related to the higher levels of the pyramid (*i.e.*, the comfort needs) is identified and as the investigation of the Eclipse plugins reveals that for the basic needs there is a large amount of research.

Table 3.1 summarizes the features of all the literature reviews and surveys discussed in this chapter. Articles have not been included, as the features included in the table do not necessarily all apply to articles.

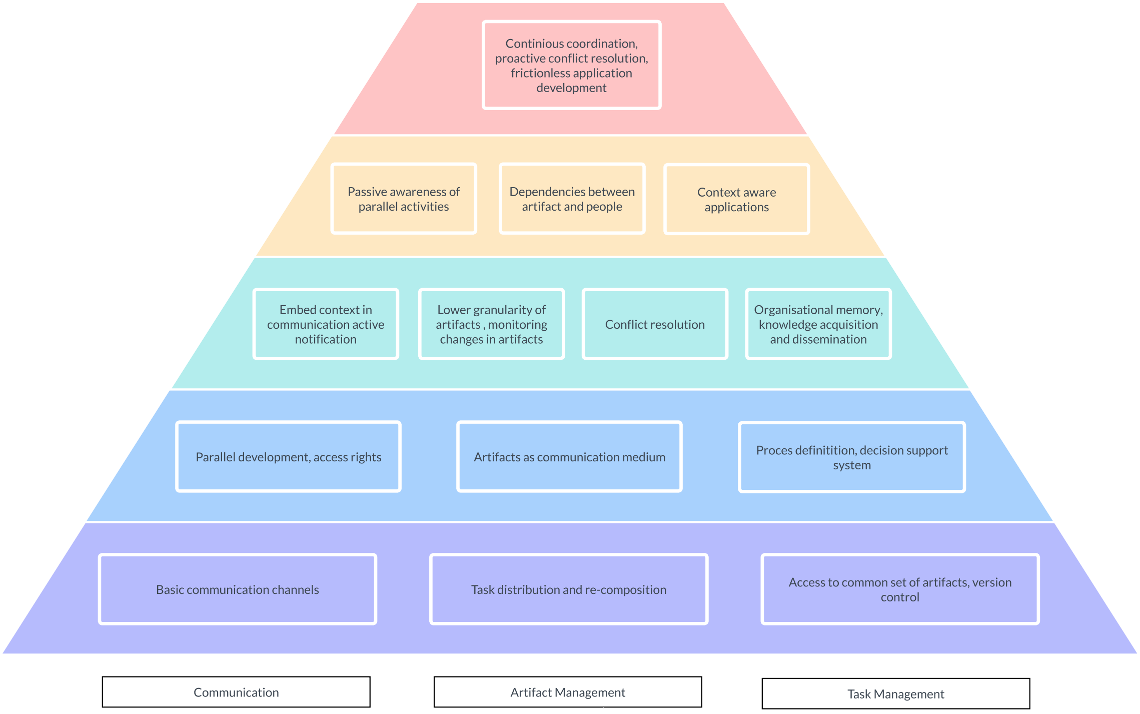

Continious coordination, proactive conflict resolution, frictionless application development
Passive awareness of parallel activities
Dependencies between artifact and people
Context aware applications
Embed context in communication active notification
Lower granularity of artifacts , monitoring changes in artifacts
Conflict resolution
Organisational memory, knowledge acquisition and dissemination
Parallel development, access rights
Artifacts as communication medium
Proces definitition, decision support system
Basic communication channels
Task distribution and re-composition
Access to common set of artifacts, version control
Communication
Artifact Management
Task Management

Figure 3.1: Collaboration Pyramid
Adapted from [59] The pyramid shows a classification framework for collaboration. The base of the pyramid consists of the basic needs, the next two layers are enhanced needs, and finally, the top two layers represent comfort needs.

Chapter 4

Methods and Taxonomy

Due to the nature of the work an initial exploratory phase was conducted where the literature was surveyed in order to gain an understanding of the broader topic. This was followed by a second phase where the addressed topics were investigated in more detail.

The methodology used in this work is based on the information and structure proposed in [56], more specifically, the systematic review process and all its phases, an overview of which is given in Figure 4.1. Given the goals of this work are to survey the available knowledge and synthesize it to produce a taxonomy; the methodology for a mapping study was used. The end result shall not only be to categorise, but also to identify areas where there is a lack of studies, or scope for further review and potentially research.

[62] identifies three phases for a review. Firstly, there is the *Planning Phase*, addressing the task of how the study should be performed. This phase involves specifying the research questions which are to be addressed, developing and validating a protocol.

The second phase is *Conducting* the review, putting the plan into action by following the research protocol developed in the planning phase. Divergences between the protocol and the reality might occur, requiring a change of plan; these changes need to be carefully documented. Conducting the review includes searching and identifying relevant literature, selecting studies, extracting the data and synthesising the information [56], [62]. Finally, the *Documenting* phase includes the reporting of the protocol and outcome. In the context of this thesis, it represents this report [56], [62]. The phases, including sub phases, are illustrated in Figure 4.1.

4.1 Planning Phase

In regard to this work, the research questions were specified in collaboration with the thesis advisor and are discussed extensively below (*cf.*, Subsection 4.1.1). The questions were formulated in such way to guide the research in covering the goals of the thesis. The aim of this study is to provide an overview of collaborative and cooperative aspects being leveraged in cybersecurity activities and create a taxonomy to categorise the approaches

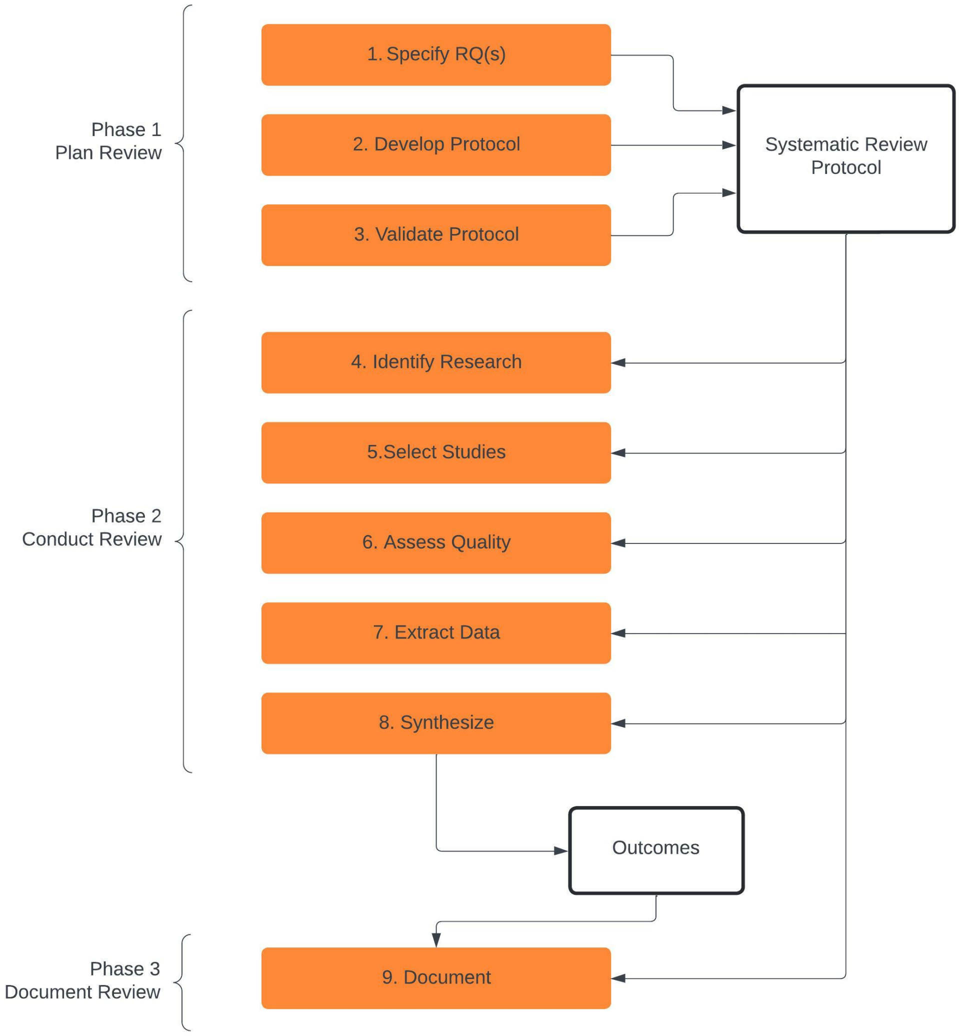


Figure 4.1: The Systematic Review Process [56]

that have been investigated. However, it is worth mentioning that for mapping studies, research questions tend to be broader and are concerned with classifying the literature hence the questions can change as the review progresses and new categories emerge [56].

4.1.1 Research Questions

This mapping study aims to understand the landscape of cybersecurity, cooperation and collaboration, as well as to understand the roles that collaboration and cooperation are playing for the application of activities in this landscape. This is followed by proposing a taxonomy which can be used to categorize the existing collaborative and cooperative approaches. Finally, based on the categorization above, a survey of existing literature is conducted. As a consequence, the initial research questions were:

- *QI* → What is the current literature landscape on the topic of cybersecurity, collaboration and cooperation?

- *QII* → Can patterns and directions be identified in the literature?

- *QIII* → What taxonomy should be used to categorise the information discovered for QII?

The research questions are ordered from the more generic to more specific. The first one is a very broad research question focused on understanding the current landscape of research. While QII and QIII become progressively more specific into the direction of providing a taxonomy and clearer direction.

Mapping studies usually have research questions that are broader in scope as they are concerned to classify the existing literature. This leads to questions that might change as the review progresses and new categories emerge [56].

Upon partial review of the literature the questions were modified, and the final versions can be found below.

- *Q1* → What interactions between cybersecurity and collaboration and cooperation have been investigated so far?
- *Q2* → Can any patterns be found in the existing literature on collaboration and cooperation in the context of cybersecurity?
- *Q3* → What taxonomy should be used to categorise the information discovered for Q2?
- *Q4* → How can the existing literature be classified based on the proposed taxonomy?

4.1.2 Protocol Development

[56] identify the main components of a protocol. Firstly a *background* section is necessary to justify the need of the research, and to summarise related concepts and related work. Within this report this information is covered in *cf.*, Chapter 2 and *cf.*, Chapter 3. A next component is specifying the *research questions* as these drive the later stages of the review process (*cf.*, Subsection 4.1.1). The *search strategy* has to be defined as a next step - this is thoroughly explained in 4.2.

As a next step of the protocol, *data extraction* decisions must be made, in particular, how the extraction and validation will be performed. The data shall include the information needed to answer the research questions as well as publication details for each paper. The *data synthesis* section of the protocol details the strategy for summarising, comparing and combining the findings of the studies used in the review. *Limitations* have to be documented as well. Finally, the *reporting* which is constituted of this report is the final step of the protocol development.

4.2 Conducting Phase

Phase two, may be performed iteratively with the classification scheme being revised as more knowledge about the topic is gained through the extraction and aggregation process. Specifically, for this paper, steps four and five from Figure 4.1 - identification of research and selection of studies were performed four times. Firstly, for the author to have a broad understanding of the existing literature about cybersecurity, collaboration and cooperation in the context of cybersecurity. Due to the unstructured nature of the first search, sources used were diverse: academic papers, book chapters and online articles. Secondly, a search was conducted to identify directions in the literature, this search was more focused, and the literature sources were limited to digital databases. The purpose was to be able to propose a taxonomy that was useful and could provide a framework for the existing work. The third search was structured and aimed to identify and select studies that would be later assessed - this search is discussed in more detail below (*cf.*, Subsection 4.2). The next steps involved extracting any synthesizing data - the results can be seen in the taxonomy created and the findings discussed (*cf.*, Chapter 5). Finally, the fourth search was based on the proposed taxonomy and searched literature on specific topics using both automated search and the backwards snowballing technique.

Search Process

For searching relevant literature three methods have been used. Firstly, a set of articles serving as a model was discussed at the beginning of the project with the supervisor. Consequently a*Manual Search* was performed *i.e.*, a number of articles was obtained non methodically. Some articles were found by searching Google Scholar others by manually searching for references in other articles.

Table 4.1: Search Strings and Number of Results

Keywords	Elsevier	IEEE Xplore	ACM	Wiley
Cy. AND Collab.	2,316	235	186,906	1,890
Cy. AND Collab. AND Identify	2,097	34	1,286	1,627
Cy. AND Collab. AND Protect	1,392	18	881	1,373
Cy. AND Collab. AND Detect	1,272	18	842	1,038
Cy. AND Collab. AND Respond	1,156	4	663	1,075
Cy. AND Collab. AND Recover	471	2	296	721
Cy. AND Coop.	1,792	84	75,211	1,289
Cy. AND Coop. AND Identify	1,577	10	708	1,110
Cy. AND Coop. AND Protect	1,159	9	536	1,026
Cy. AND Coop. AND Detect	915	7	480	792
Cy. AND Coop. AND Respond	945	3	383	760
Cy. AND Coop. AND Recover	415	1	216	535

Cy. = Cybersecurity, Collab. = Collaboration, Coop. = Cooperation

A second type of search was the *Automated Search* which involves a number of search strings being defined as shown in Table 4.1 and used to search in the following digital databases:

- IEEE Xplore
- ACM Digital Library
- Wiley Online Library
- Science Direct/Elesvier

Finally, *Snowballing* refers to a search technique that identifies further studies relevant to the systematic literature review from the existing ones [56], [62]. It is complimentary to manual and automatic search and requires an existing set of papers, to serve as starting point. The papers need to be known as relevant. The rationale of the technique is that relevant papers will reference other relevant papers to the specific subject, hence additional papers which were missed in the initial search might be found [62]. Two snowballing techniques exist: *Backwards snowballing* refers to a search based on the reference list of papers that are known to be relevant [56]; and *Forwards snowballing* refers to the technique whereby all papers that cite a known paper are found [56]. In this work only backwards snowballing was used sporadically to identify further papers.

Table 4.1 shows the keywords used in the search and the number of available papers. During the first two searches detailed above, only the combinations *Cybersecurity AND Collaboration* and *Cybersecurity AND Cooperation* were used. Subsequently, once the taxonomy framework was created, the search was restricted by including the five NIST functions in the search string. As the number of papers was still very large the following

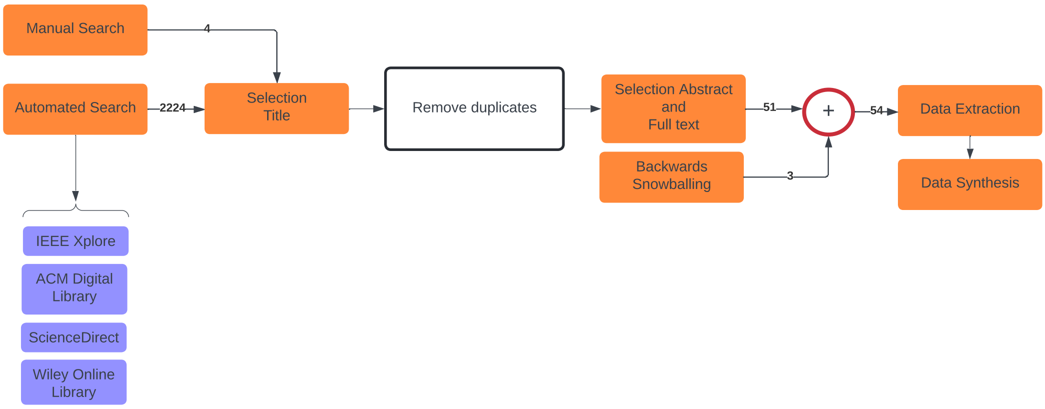


Figure 4.2: Conducting the review: detail on the search and selection processes

strategies were employed. For the IEEE Xplore results *only*, all papers were assessed for relevance. For the other three databases, only the first 100 papers were assessed - the search was sorted by relevance as defined in the corresponding search database.

The final search was performed after the taxonomy was completed and focused on areas of interest based on the taxonomy. The focus was on three identified topics:*(i)* Collaborative or Cooperative Access Control *(ii)* Collaborative or Cooperative Intrusion Detection Systems *(iii)* Collaborative or Cooperative Information and Vulnerability Sharing. This search included backwards snowballing, as the references of already identified papers were searched for further literature, and an unstructured automated search in the four databases discussed previously.

Selection Process

The selection process was applied to all the results of the search in order to determine which studies shall be used for the review. Exclusion criteria were: *(i)* literature published in a different language than English *(ii)* works published before 2007 *(iii)* literature not available as open access, which often included book chapters.

Table 4.2: Data Extraction Template

Standard Bibliography Data: Publication year, author, title etc
Cybersecurity and Collaboration and Cooperation interaction
NIST Function
NIST Category
Findings
Synthesis of the points above for the Findings chapter

The selection approach was based on three steps. Firstly, on the basis of the title - for a lot of the search results the title was already a good indication that the works were not

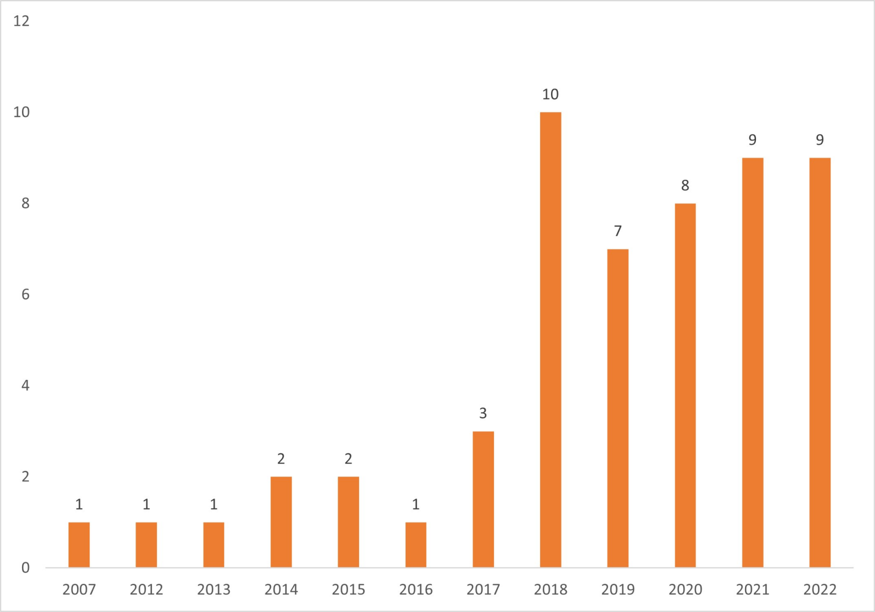


Figure 4.3: Distribution of selected papers by year

relevant for this thesis. For example, the literature where collaboration and was not the focus but rather a secondary aspect. The domain was far removed, or very specific in an area unfamiliar to the author of this project. Secondly, the selection was performed on the basis of the abstract. Once the first set of searched papers was excluded, the abstract of all papers was read and based on the information in the abstract, another set of papers was excluded. Finally, for the remaining papers, an examination of the full text was performed to select the final set of papers. These can be seen in Table 4.3. The entire selection process including the numbers of papers selected at each step are detailed in Figure 4.2 this refers to the third and fourth search. The initial manual search consisted of 4 papers, while the automated search consisted of a total of 2224 papers. A very large number of these were duplicates.

Regarding the distribution across years, Figure 4.3 provides an overview of the distribution of the selected papers across the years. The trends in literature will be further examined in the Findings chapter (*cf.*, Chapter 5).

Data Extraction and Synthesis Process

The selected papers were read by the author and the data was extracted during June, July and August 2022. The template used to extract data is shown in Table 4.2. It shows what information was extracted from the selected papers. Publication information was extracted for each paper, both as a way to organise the information, and to identify trends based on year of publication. The interactions between cybersecurity, collaboration and cooperation information were extracted to find out how the papers fit in the scope of this thesis. The NIST Function and Category was identified for each piece of literature to classify it in the taxonomies. Findings were extracted and summarised.

The aim of the data synthesis was twofold: firstly, to provide a meaningful taxonomy for classifying papers on the topic of cybersecurity and collaboration or cooperation, and to survey the existing literature while using the proposed taxonomy to classify it. A challenge encountered during the synthesis process was that different authors use different terminology for the same concepts or use specific terms interchangeably. Particularly difficult given the scope of this work was the use of cooperative and collaborative interchangeably in a number of papers.

Table 4.3: Selected Papers

	Year	Title	Authors	Topic
1	2017	Cybersecurity Cooperation of Countries: Impact of Draft International Code of Conduct for Information Security	G. Lkhagvasuren	International Cy. Coop.
2	2016	Shall We Collaborate?: A Model to Analyse the Benefits of Information Sharing	R.Garrido-Pelaz et al.	Information Sharing
3	2021	Continuous User Authentication for Human-Robot Collaboration	S.S. Almohamade et al.	Continious User Authentication
4	2020	Cybersecurity Event Detection with New and Re-emerging Words	H.Shin et al.	Vulnerability Disclosure
5	2022	Anomaly Detection in Cybersecurity Datasets via Cooperative Co-evolution-based Feature Selection	A.N.M.B Rashid	Vulnerability Disclosure
6	2021	Vulnerability disclosure and cybersecurity awareness campaigns on twitter during COVID-19	A. Bahl et al.	Vulnerability Disclosure
7	2022	Collaboration and advance planning across campus create more cybersecure universities	M. Bannister	Campus Cybersecurity
8	2017	Bring the State Back In: Conflict and Cooperation Among States in Cybersecurity	Y.Cho	International Cy. Coop.
9	2019	Machine learning in cybersecurity: A review	A.Handa	Intrusion Detection
10	2017	Perspectives on Cybersecurity Information Sharing among Multiple Stakeholders Using a Decision-Theoretic Approach	M.He et al.	Information Sharing
11	2022	Collaboration or separation maximizing the partnership between a “Gray hat” hacker and an organization in a two-stage cybersecurity game	D.Cohen et al.	Vulnerability Disclosure Game
12	2018	A framework for enabling security services collaboration across multiple domains	D.Migault et al.	Security Service Collab.
13	2022	Agile incident response (AIR): Improving the incident response process in healthcare	Y.He et al.	Agile Incident Response
14	2021	Cybersecurity professionals information sharing sources and networks in the U.S. electrical power industry	R.G.Randall	Power Grid Information Sharing
15	2020	Cybersecurity investments in the supply chain: Coordination and a strategic attacker	J.Simon et al.	Supply Chain Cy.
16	2022	Collaborative collision avoidance for Maritime Autonomous Surface Ships: A review	M.Akdağ et al.	Collab. Collision Avoidance
17	2020	Zombies, Sirens, and Lady Gaga – Oh My! Developing a Framework for Coordinated Vulnerability Disclosure for U.S. Emergency Alert Systems	A. Woszczynski et al.	National Cy. Coop.
18	2021	Worm computing: A blockchain-based resource sharing and cybersecurity framework	L.Shi et al.	Worm Computing
19	2021	Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management	R.Rajan et al.	Strategic Cy. Management
20	2020	Governance of Collaborative Networked Organisations: Stakeholder Requirements	T.Tagarev	Collaborative Networked Organisations
21	2019	Cybersecurity Culture in Computer Security Incident Response Teams	M.Ioanniu et al.	Collab. Culture Governance
22	2022	Cybersecurity Vulnerability Identification in System-of-Systems using Model-based Testing	M.M.Thwe et al.	Vulnerability Identification
23	2019	SeArch: A Collaborative and Intelligent NIDS Architecture for SDN-Based Cloud IoT Networks	T.G. Nguyen et al.	Intrusion Detection
24	2013	Information Sharing Models for Cooperative Cyber Defence	J.L. Hernandez-Ardieta et al.	Information Sharing
25	2021	Information Sharing Models for Cooperative Cyber Defence	D.Zhuravchak et al.	Honeypots

Continued on next page

Table 4.3 – continued from previous page

	Year	Title	Authors	Topic
26	2020	Interactive Machine Learning for Data Exfiltration Detection: Active Learning with Human Expertise	M.H.Chung et al.	Data Exfiltration
27	2019	Privacy Preserving Cyber Threat Information Sharing and Learning for Cyber Defense	Badsha et al.	Information Sharing
28	2019	ExSol: Collaboratively Assessing Cybersecurity Risks for Protecting Energy Delivery Systems	J.Lamp et al.	Collab. Risk Assessment
29	2018	Early Detection of Cybersecurity Threats Using Collaborative Cognition	S.Narayanan et al.	Collab. Cognition
30	2018	Osmotic Collaborative Computing for Machine Learning and Cybersecurity Applications in Industrial IoT Networks and Cyber Physical Systems with Gaussian Mixture Models	E.Oyekanlu	Collab. Computing
31	2020	Resolving the cybersecurity Data Sharing Paradox to scale up cybersecurity via a co-production approach towards data sharing	A.Atapour-Abarghouei et al.	Data sharing
32	2021	Research on Internet of Vehicles Attack Prediction Based on Federated Learning	L.Tang et al.	Intrusion Detection
33	2021	Detecting and Preventing Faked Mixed Reality	F.Kilger et al.	Virtualised Collab.
34	2019	Privacy-Preserving Collaborative Data Anonymization with Sensitive Quasi-Identifiers	K.S. Wong et al.	Data Anonymisation
35	2022	Cooperative Location-Sensing Network Based on Vehicular Communication Security Against Attacks	Z. Wang et al.	Coop. Location Sensing
36	2022	ADS-Lead: Lifelong Anomaly Detection in Autonomous Driving Systems	X.Han et al.	Anomaly Detection
37	2018	Learning from experts' experience: toward automated cyber security data triage	C.Zhong et al.	Incident Response
38	2014	HosTaGe: a Mobile Honeypot for Collaborative Defense	E. Vasilomanolakis et al.	Honeypots
39	2022	Challenges in the safety-security co-assurance of collaborative industrial robots	M.Gleirscher et al.	Collaborative robots
40	2015	Controlled data sharing for collaborative predictive blacklisting	J.Freudiger et al.	Data Sharinig
41	2018	DDoS Defense using MTD and SDN	J.Steinberger et al.	Moving Target Defense
42	2012	A collaborative information sharing framework for community cyber security	W.Zhao et al.	Information Sharing
43	2015	Mitigating risk with cyberinsurance	P.H.Meland et al.	Cyberinsurance
44	2017	SVM-DT-based adaptive and collaborative intrusion detection	S.Teng et al.	Intrusion Detection
45	2018	Developing collaborative and cohesive cybersecurity legal principles	J.Kosseff	Legal Cy. Framework
46	2019	An attribute-based controlled collaborative access control scheme for public cloud storage	Y.Xue et al.	Access Control
47	2007	Prevention, detection and recovery from cyber-attacks using a multilevel agent architecture	D.Edwards et al.	Intelligent Software Agents
48	2001	Activity Control Design Principles: Next Generation Access Control for Smart and Collaborative Systems	J.Park et al.	Access Control
49	2018	Collaborative access control of cloud storage systems	Y.H.Chen et al.	Access Control
50	2019	Cyberthreat-intelligence information sharing: Enhancing collaborative security	M.Liu et al.	Vulnerability Sharing
51	2014	Enhancing big data security with collaborative intrusion detection	Z.Tan et al.	Intrusion Detection
52	2020	Behaviour-Based Biometrics for Continuous User Authentication to Industrial Collaborative Robots	S.Almohamade et al.	Continious User Authentication
53	2022	CoReTM: An Approach Enabling Cross-Functional Collaborative Threat Modeling	J.von der Assen et al.	Collab. Threat Modeling
54	2020	Predictions of network attacks in collaborative environment	M.Husak et al.	Attack Prediction

Chapter 5

Findings

The world is increasingly interconnected, leading to an increase in cyberattacks. From 2017 to 2018 public and private sector organisations saw a rise in the average number of security breaches from 130 to 145 [1]. Furthermore, with the increase of attacks, the resolve times is longer and the cost of cybercrime increases. During the same period, 2017 to 2018 the average cost of cybercrime for organisations rose by 12 per cent to USD13 million. The covid pandemic accelerated the rise in cyberattacks even more [63]. In March 2020 there was a 600 percent increase in phishing attacks and between January and April 2020, in the timespan of only 4 months, Interpol detected around 907,000 spam messages, 737 malware-related incidents, and 48,000 malicious URLs all tied to COVID-19 [63]. This is consistent with the findings of World Economic Forum (WEF) [64] who find that cyberattacks and data fraud due to sustained shift in working patterns are one of the most concerning topics in the world. This is based off a survey among risk professionals and professional networks of Marsh McLennan Companies (MMC) and Zurich Insurance Group (Zurich). Finally, the Federal Bureau of Investigation (FBI) published the losses due to internet fraud to be USD6.9 billion in 2021.

It seems therefore that cybersecurity is an extremely relevant topic, which is why many governments and organisations are putting increasing effort into the topic. Multiple frameworks have been proposed in the last years to tackle cybercrime. The Swiss Government has set up a National Cyber Security Center in July 2020 [65] and among the current topics listed are a number of cybersecurity subjects, including cooperation. Collaboration and cooperation, particularly related to sharing of vulnerabilities, feature in multiple principles and recommendations from the Department of Homeland Security in the U.S. [66], the European Union [67] and others [68].

The NIST cybersecurity framework was already introduced in Subsection 2.1.6, a more detailed explanation is provided here. The *Identify* function refers to identifying an inventory of critical cyber assets (CCAs) and developing procedures, policies and a fitting governance for the organisations to manage cybersecurity risks to all assets, data, systems and capabilities. The Categories belonging to the Identify function, are *Asset Management*, *Business Environment*, *Governance*, *Risk Assessment*, *Risk Management Strategy*, *Supply Chain Risk Management* [6], [69]. The Identify Function is not concerned with the identification of attacks.

The *Protect* function is concerned with protecting assets through the introduction of cyber protection techniques. It includes the following categories *Identify Management and Access Control* to limit access to authorised users only. *Awareness and Training* preparing personnel to perform security related duties, *Data Security* managing information and data according to the risk strategy of the organisation. *Information Protection Processes and Procedures*, *Maintenance* and *Protective Technology* complete the categories [6], [69].

The actual identification of attacks and detection of malicious cyber activity is included in the *Detect* function. Here emphasis is placed on timely discovery of *Anomalies and Events. Security Continuous Monitoring* refers to monitoring the assets and systems at discrete time intervals to detect events, and finally, *Detection Processes* is the third category in this function [6], [69].

The fourth NIST function is *Respond* and is concerned with the reaction to a cyberattack by developing appropriate processes when the Protect and Detect functions fail to prevent an attack. The Respond function aims to minimise impact of the attack the five categories belonging to this function are: *Response Planning*, *Communication*, *Analysis*, *Mitigation*, *Improvements* through the incorporation of knowledge acquired thanks to the latest attack [6], [69].

Recover, the final function, refers to recovering and returning everything to normal operation while reducing the impact of the event. Categories of this function are *Recovery Planning*, *Improvements*, *Communication.* Note that both the Respond and Recover functions have Communication and Improvements categories making the classification more difficult [6], [69]. Figure 5.2 provides an overview of the various functions discussed above and the categories belonging to each function.

5.1 Taxonomy based on NIST Framework

Given the relevance of cybersecurity nowadays, it seems fitting to look at the topic from the perspective of collaboration or cooperation in this context. The NIST framework is widely used across corporations, with the predicted usage in 2020 reaching 50 percent across the U.S. [61], while the usage in 2012 was at 0 percent and in 2015 at 30 percent. It is safe to assume that if the trend is followed, more than half of all U.S. organisations will use the NIST framework by now. One of the reasons is the fact that NIST is an American standard, whereas in Europe, standards by the International organisation for Standardization(ISO) are more widely accepted. However, due to its simplicity and breadth of usage, the taxonomy proposed in the following section is based on the NIST framework. A further reason to use NIST is that based on the surveyed literature, more papers cite the NIST framework or NIST-alike frameworks as opposed to ISO [48], [70].

The research published on collaboration and cooperation in cybersecurity is very diverse, ranging from studies trying to identify factors which are related to the development of a cybersecurity culture across an organisation and the difficulties faced regarding the communication and collaboration on the topic [71] to much more technical approaches such as collision avoidance algorithms for autonomous ships, and in particular the exchange of

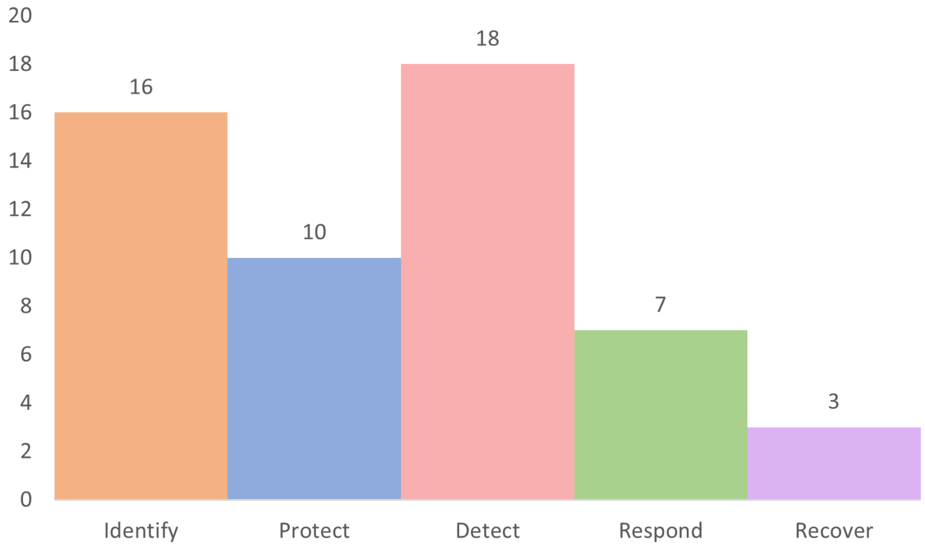


Figure 5.1: Literature classification based on the NIST Framework

information and interactions between ships [72]. Therefore, as the 5 categories of the NIST framework are exhaustive and diverse enough to be able to cover most of the literature, they are used for an initial taxonomy.

It is worth to note that some papers can be categorized as belonging to multiple functions. For example, if one is tackling both topics related to the detection of cyberattacks, and to the communication and mitigation in the future, the approach taken is always to include a paper in one category only, and the motivation for each decision is provided in the next section.

Figure 5.1 provides an overview of the split of literature belonging to each NIST function. It is interesting to note that the distribution is similar to the number of papers identified during the search for particular keywords (*cf.*, Table 4.1) with one notable outlier, the Detect function. This outlier can be explained by different terminology. The term identify intuitively means identifying an attack, however in the context of NIST the actual identification of attacks belongs to the Detect function, while Identify refers to identifying assets etc. that need to be protected. Therefore, the Detect function benefitted from the search both of the keywords ”Identify” and ”Detect” and therefore more results were found.

5.2 Literature Review

This section provides a summary of all the papers used for creating the taxonomy. Where a paper could belong to more than one NIST Function, an explanation is provided as to why the specific categorisation was decided. Furthermore, the NIST framework provides in addition to the main five functions, several categories and subcategories. A category was provided for every single inspected paper, for those covering more than one function, a second category is provided as well. Subcategories are not provided, they are very specific and numerous, 108 subcategories exist, their use would go beyond the scope of this work. Based on the number of identified papers at most half the subcategories would be used.

5.2.1 Identify

As the United Nations (UN) has defined cybercrime a type of transnational organised crime [73] many countries have proposed various cybersecurity frameworks and policies. 76 countries have approved cybersecurity strategies which involve international cooperation to tackle cybercrime [73] with key players being the following: U.S., China, Russia Japan, Republic of Korea, Estonia, India and Australia. Additionally regional and international organisations are working on initiatives to combat cybercrime. The Association of Southeast Asian Nations (ASEAN) created a working group on cybercrime in 2014 already. While the G7 proposed in 2016 the "G7 Principles and Actions of Cyber". These steps all aim to create an environment of policies, procedures and processes to improve cybersecurity, but also raise awareness of threats and of the importance of a suitable security.

A contrasting perspective to [73] is provided by [74]. Here, the authors highlight the expansion of conflict between states in cyberspace. Comparing the global cyberspace to other security spaces around the world, it highlights its anarchic system with no absolute authority or institutional power. Therefore, various states will try to create systems favourable to themselves, based on cyber sovereignty and cyber power. Because cyber power has both material and non-material aspects, and states cannot effectively assess the power of other states conflicts in the cyberdomain are intensifying.

[74] finds that the countries which most actively compete for the upper hand in cyberspace are the U.S. and China, but it also acknowledges that the competition invites cooperation among the states in addition to conflict. [74] discusses cooperative endeavours between Russia and China with the aim to encourage cooperation with developing nations and support them technologically in the fight against cyberattacks. The U.S. and a number of European countries joined NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) focusing on military cooperation for cyber defence technical development. However, the conclusions of the authors are that despite the fact that there was emphasis on inter-state cooperation in cybersecurity, this cooperation will likely be temporary as states regard domestic policy and strategy of higher importance than international cooperative organisations.

The two contrasting views above tackle collaboration on international and governmental level highlighting the importance of collaboration and cooperation on the cybersecurity front. As they are concerned with the broader picture in which governments and organisations operate, they are included in the Governance category, with Business Environment serving as second category.

Looking at security on a national level, the Emergency Alert System (EAS) [75] in the U.S. is a public warning system that permits important information to be communicated to the public - this includes extreme weather conditions, wildfires or any other emergency alerts. Although of critical importance, it runs on legacy software and has limited cybersecurity

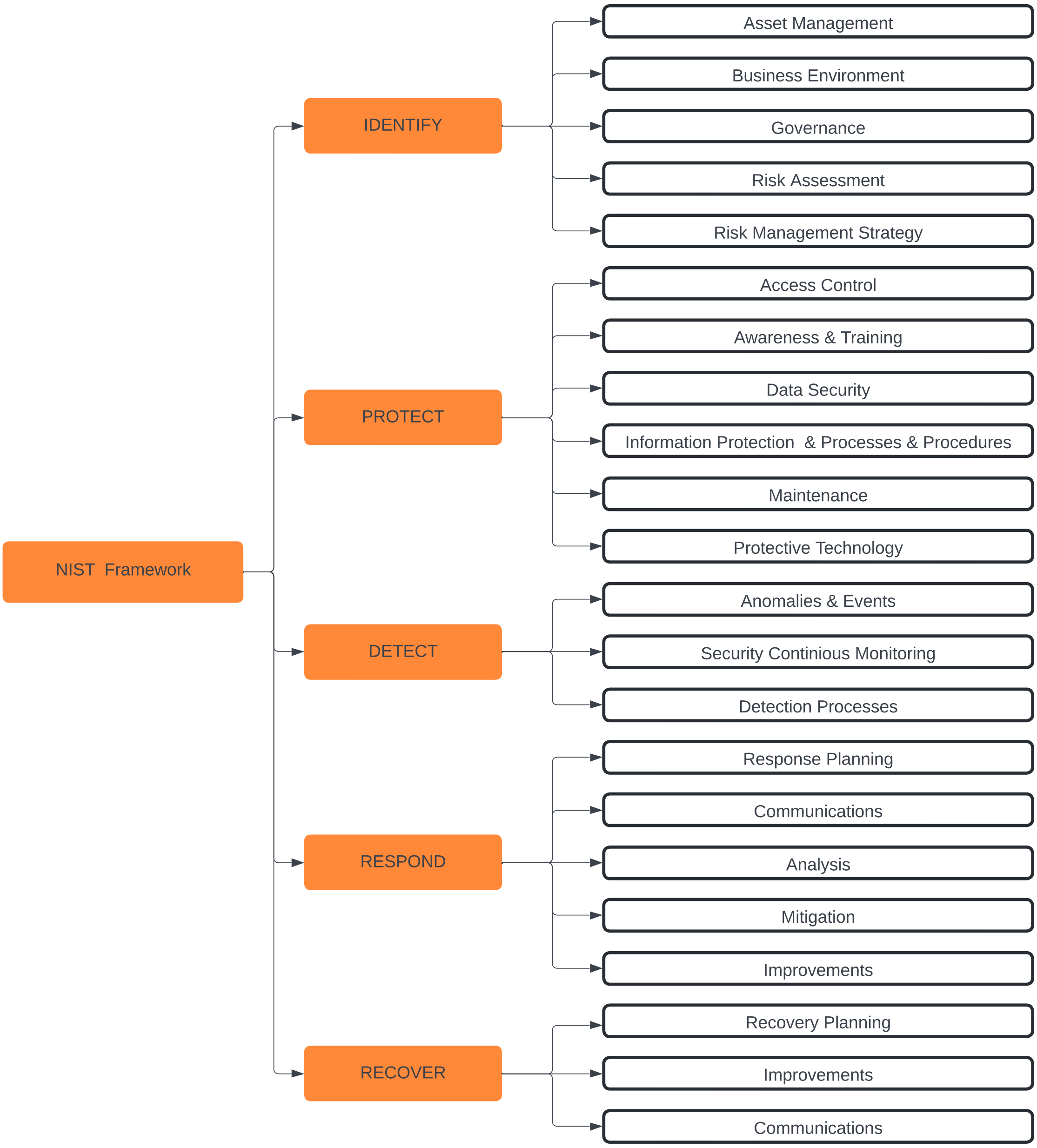


Figure 5.2: NIST Framework

protection [76]. For instance, the EAS shared a video of Lady Gaga instead of an actual alert notification in 2011 and in 2013 it warned of a zombie apocalypse. These are just a couple of incidents that arose from the lacking cybersecurity of the system.

Woszczynski et al. propose a method for engagement between EAS authorities and external researchers in the field of cybersecurity to detect, recover and disclose vulnerabilities in the system, using coordinated vulnerability disclosures (CVD) policies. The authors find that when cybersecurity researchers find vulnerabilities in systems, they fear disclosing them, because the U.S. has punishing laws - even just scanning another system without approval can be criminally punishable. Therefore, two recommendations are made: firstly, researchers should familiarize themselves well with the CVD policies of an organisation before starting to investigate its systems and try finding vulnerabilities. Secondly, the authorities should oppose laws that criminalize research into cybersecurity if no intention to harm exists and foster partnerships between the public and industry and the government itself [76]. Thus, from a collaborative perspective, it is important to design laws and processes that foster cooperation and collaboration.

Narrowing the area further, [77] looks at cybersecurity on campus and discusses the environment in which cybersecurity should operate. ”Cybersecurity is a threat that changes all the time, so addressing it involves everybody living and breathing security as second nature” [77]. Recently there have been a number of data breaches and ransomware attacks directed towards universities, and the author emphasizes the need for all stakeholders to become aware of the risks on campus and be proactive in fighting the threats. [77] proceeds with suggestions based on collaboration and advanced planning to create more secure universities. Among the recommendations are to learn who is responsible for information security on campus and engage with them to find out how everyone can help. Learning about the university incident plan and ensure individuals have a back-up of their data, while being aware where the university data is stored, are also important factors. Making sure that the CIA triad principles are upheld, with secure identification, and only giving access to data on a need-to-know basis are points to remember. Finally, educational material should be offered to both staff and students about online safety. All of these are points emphasized by the NIST Cybersecurity Framework in regard to the Business Environment - in this case the university environment. The author concludes with an important statement - conversations about cybersecurity should happen, not only after a cyberattack. In fact they should best happen *before* a cyberattack.

M. Akdağ et al. investigated collision avoidance algorithms for autonomous ships, and in particular the exchange of information and interactions between ships [72]. Building on the assumption that vessel-to-vessel communication and route exchange, as opposed to autonomous ships to an automatic identification system, can improve collaborative avoidance algorithms (CVAs). The authors found that CVAs in the maritime industry were self-contained and did little to foster collaboration and data exchange between users, while CVAs for other types of vehicles, for instance ground and air ones, were much better developed regarding the collaboration aspect. Even more importantly, in the case of aerial vehicles, the communication between vehicles is considered crucial for collision avoidance purposes. CVAs proposed so far in the maritime industry consist of optimisation algorithms aimed at finding the globally optimal solution for navigating taking into consideration spatial and temporal constraints.

In [72] an outline for a future collaborative collision avoidance algorithm is drafted. The authors consider that their method can be implemented in conventional ships but also in the emerging field of autonomous ships, as collaborative collision avoidance and route exchange will improve maritime autonomous surface ships and conventional ships navigational safety. The proposed method aims to prevent misunderstandings related to verbal communications and decision-making by the Officer on Watch will improve with the knowledge of the previously negotiated collision-free trajectories [72].

Cybersecurity management is an important aspect for every organisation, and these should learn to deal with vulnerabilities and threats through effective processes and management decision across the business [78]. Using a modified total interpretative structural modelling technique, Rajan et al. identifies the factors that affect cybersecurity within organisations and analyses the relationships among them. Subsequently the authors investigate how an effective cybersecurity management can be built based on the identified factors. A hierarchical model of factors is constructed, with governance being shown as playing the most important part in cybersecurity management. Alliances and collaboration are identified as the next most important factors. Other identified factors are training, security awareness and technological infrastructure. The above, are all factors that closely relate to the Identify step of the NIST framework. The proposed model for cybersecurity management consists of a top management that encourages alliance and collaboration with other organisations in their field, but also across the organisation itself. Trainings and knowledge-sharing discussions should be organised across teams to learn how to deal with cybersecurity threats, which can lead to information flow and security awareness [78].

Cybersecurity investments were investigated for supply chains in [79]. As cybersecurity is a challenge faced by firms who depend on other firms in the supply chain - an attack on one can have an impact on all. For example, large organisations, such as Target, T-Mobile USA or Fiat Chrysler dealt with cyberattacks because their third-party providers were compromised. Simon et al. analyse the differences between cybersecurity investments that are coordinated or uncoordinated across various organisations and the dissimilarities between strategic and non-strategic attackers. In the context of the analysis, a *strategic* attacker choose a specific organisation as a target, influenced by its investments in cybersecurity, while a *non-strategic* attacker is not influenced by the investments in cybersecurity of organisations when choosing a target.

As expected, the results show that with non-strategic attackers, nodes (firms) acting independently will underinvest in cybersecurity as they ignore the impact of attacks in the rest of the chain. Larger nodes will invest more in their security and even subsidize smaller ones, even without formal agreements. And finally, when faced with strategic attackers, the optimal investment is more disparate across the supply chain to make the attacker more indifferent of who it attacks. The more surprising finding is that overall lack of coordination leads to underinvestment, however when faced with strategic attackers independently, nodes tend to invest more than with non-strategic attackers - hoping to push attack probability to other nodes. This is, of course, most relevant, when indirect damages are rather low [79]. The paper brings some light into the complex workings of supply chain coordination and can serve as a guide to organisations on how to manage supply chain risk, consequently it is included in the Supply Chain Risk Management category.

Recently, collaborative networked organisations (CNOs) have emerged in a variety of fields [80]. Consisting of a network of organisation and people which are autonomous, heterogeneous and geographically distributed, they collaborate to achieve common goals. As CNOs are of interest for the development of competence networks for cybersecurity, T.Tagarev conducted interviews with stakeholders - funding organisations and potential customers of cybersecurity solutions - to identify governance needs and objectives for CNOs and prioritize them.

The findings show that an important concern for all the stakeholders is the geographic representation of the countries involved in the networked organisation, however despite the perceived importance the views were contradictory *i.e.*, some respondents preferred national collaboration while others international/European collaboration, certain respondents were concerned to open EU-centred networks for cybersecurity to Eastern countries, without defining what Eastern exactly represents in the context. Furthermore, important aspects identified for the governance of CNOs are involvement of external stakeholders, the decision-making agreements and the need for confidentiality. Another aspect of the CIA triad (*cf.*, Subsection 2.1.2), integrity, as well as accountability were also identified although not of as high priority as confidentiality. The research serves as a basis for development of governance models in the context of the European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO) projects.

[81] argues that the increasing complexity of cybersecurity and globalization makes it impossible for organisations to manage cyber-threats and-incidents alone, without collaborating with any partner. In [81] it is argued that successful policies for sharing information near real time, must be based on two pillars at least. Firstly, the development of formal models to estimate the value of the information shared is needed; secondly, models assessing the trust and reputation of community members need to be identified. As such, the authors propose a formal model of information sharing communities and an information sharing algorithm. Analysing the process of sharing using a topology method, the community and the information network are modelled. The authors shed some light on factors that can be inhibiting for the spread of information sharing communities and what could deter members to actively participate in information sharing once already a part of a community.

A further look at information sharing communities is proposed by [82]. The paper discusses a collaborative information sharing framework for community cybersecurity. In the context of this work, the authors define communities as public and private entities in a geographical region, including government, industry - finance, healthcare, utilities - and academic organisations. Referring to the good collaboration among government departments, Zhao et al. note that this is lacking across other organisations and sectors of a community - despite the usefulness of collaboration and the difficulty of single organisations to identify and detect cyber threats alone.

Similarly, to the work by [83] discussed later, which looked at how much data sharing is ”just enough” to be useful but to not disclose too much information, [82] asks the following questions: (1) What information should be shared? (2) Who should it be shared with? (3) When should it be shared? (4) How should it be shared to endure an effective and secure transfer? To answer these questions, the authors propose a collaborative informa-

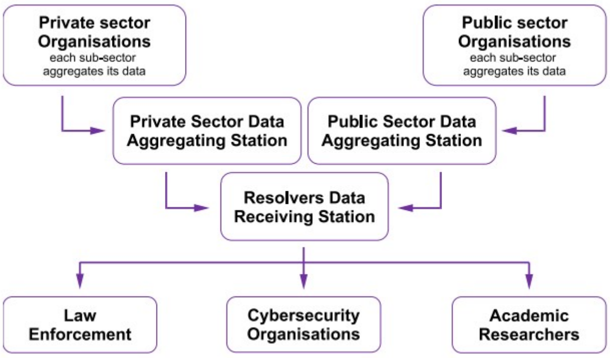

Private sector Organisations
each sub-sector aggregates its data
Public sector Organisations
each sub-sector aggregates its data
Private Sector Data Aggregating Station
Public Sector Data Aggregating Station
Resolvers Data Receiving Station
Law Enforcement
Cybersecurity Organisations
Academic Researchers

Figure 5.3: Network of third party owned data aggregating stations [86]

tion sharing framework designed specifically for communities. Communities are divided in three groups: sector groups - facilitating information sharing between organisations in the same sector, non-sector groups - facilitating information sharing between organisations that do not belong to any major sector and super groups - usually comprised of cybersecurity domain experts, coordinate with the various sector, non-sector and external sources such as other communities.

A second division is possible, in collaboration groups - which aim to be long term structures dealing with routine information sharing and incidents that relate to all members of the community (*cf.*, Subsection 2.2.1) and incident groups - dynamically established groups operating together for a limited time to support incident-specific sharing of information. The discussion of types of groups and how collaboration can be achieved leads to the inclusion in the governance category of the Identify function. The paper does however cover challenges related to information sharing for community cybersecurity, as such all functions of the NIST framework are covered.

Cyberattacks on Energy Delivery Systems (EDS) - the power grid, oil and gas industry, etc. - are a serious threat and can result in large economic losses, among others [84]. For instance, in 2015 the Ukrainian power grid was hacked, leading to power outages lasting for hours for close to a quarter million consumers in Ukraine [85]. The diversity as well as interdependency of Energy Delivery Systems makes it difficult to perform risk analysis, and the increasing number of attack vectors complicate the task even further. J.Lampe et al. propose a risk-assessment framework which is requirements-based, collaborative and real-time. The framework comprises the following: *(i)* an approach to model real-life EDS infrastructures, *(ii)* an approach to retrieve, query and model security requirements for EDS and *(iii)* a methodology for risk calculation both for a single asset and system wide. The proposed framework was evaluated experimentally to see how it reacts in realistic attack scenarios. Due to the aim of the work [84] to help collaborators to reach decisions together about the protection as well as the mitigation actions suitable for their infrastructure, this work was included in the Identify function.

A closely related topic to the model EDS and risk calculation methodology addressed in [84]is introduced in [37]. The authors propose a collaborative methodology-based approach for tackling threat modelling within organisations. A method comprised of identifying the potential assets which need to be protected and the potential attack vectors that can be used for the asset, threat modelling is an established method to design more resilient systems and networks. Acknowledging the increase in remote work in the last years, the proposed solution enables collaboration for stakeholders which are located remotely, on-site or use a hybrid approach. Moreover, the solution is aimed at stakeholders with different backgrounds and knowledge areas. The solution proposes an editor to model assets and threats flexibly. A questionnaire is then used to decide on one of the available methodologies, based on which the collaborators are guided through the threat modelling process. The emphasis of identifying assets needing protection and possible threats led to the inclusion of this paper to the Identify section.

A.Atapour-Abarghouei et al. propose a co-productive approach to data collection and sharing to respond to cybercriminals that continuously scale up their operations to increase profits [86]. The approach proposed is to overcome the cybersecurity data sharing paradox - similarly to other paradoxes discussed in this paper, where organisations agreed on the need for better information sharing, but were deterred to actually share internal information, the core of this paradox is the understanding that private and public interests differ from each other. Law enforcement and industry have different approaches to the issue of cybersecurity, and consequently they have different approaches to solving these issues in their own interest. This difference manifests itself in different practices for data sharing between each other as well as with other parties, such as security analysts or cybersecurity researchers. The authors argue that a few operational models containing good practices exist and can provide a good solution. Consequently, A.Atapour-Abarghouei et al. propose a solution of organising co-productive data collections on the basis of different sectors while emphasizing the need for common standards for collection of data. Ideally, data should be aggregated along the lines shown in Figure 5.3 and all involved parties should collaborate with each other.

Crises such as the COVID-19 pandemic highlight the usefulness of virtualized collaboration, which can increase the remote management of critical infrastructure [87]. Mixed reality(MR) enables the remote management in a wide range of fields: energy systems, medicine and education, among many others. However, by design mixed reality is a false reality generated from models - making the detection of attacks particularly difficult. Many attacks related to MR are due to well-known threats. Kilger et al. provide an overview of attack vectors and surfaces, as well as concrete threats which are relevant in the context of mixed reality. Finally, a number of features are introduced that can help with the detection of fake MR. Due to the exploratory character of this paper, and its discussion of potential attacks and mitigating aspects, it is included in the Risk Assessment category.

A relatively rarely discussed topic related to cybersecurity is cyberinsurance. This concept refers to the ”transfer of financial risk associated with network and computer incidents to a third party” [88]. To facilitate transfer of risk, Meland et al. cite one of the most important challenges related to cyberinsurance to be translating the cybersecurity risks into numbers. The task lays both with the insured and insurers and is one of many issues on which the two collaborate. Firstly, information on past attacks becomes outdated rapidly with the technological development and advancements of attacks. Secondly, standardizing cyberinsurance is a challenge - as an example, ransomware attacks do not classify as

Table 5.1: Papers on the Identify Function

Work	Year	Category	Secondary Category
[73]	2017	Governance	ID - Business Environment
[74]	2017	Governance	ID - Business Environment
[77]	2022	Business Environment	-
[79]	2020	Supply Chain Risk Management	-
[72]	2022	Risk Assessment	-
[76]	2020	Governance	-
[78]	2021	Asset Management	-
[80]	2020	Governance	-
[81]	2013	Governance	DE - Anomalies and Events
[84]	2019	Risk Assessment	ID - Risk Management Strategy
[86]	2020	Business Environment	-
[87]	2021	Risk Assessment	DE - Anomalies and Events
[82]	2012	Governance	PR, DE, RS, RC
[88]	2015	Governance	RS - Mitigation
[89]	2018	Governance	ID - Supply Chain Risk Management
[37]	2022	Asset Management	ID - Risk Assessment

theft, as the files that are encrypted during an attack are still on the victim's drive, Furthermore, as seen in [90], it can take quite a while to discover breaches, and even longer until the breaches are resolved or patched. There might pass even more time until the organisation sees what the real damage and effects of the breach were. Therefore, the ideal time to sign a policy is before an exploitable vulnerability even exist, but how to know exactly when that is, is a challenge in itself.

All these issues, including the unknown or known presence of vulnerabilities, impact the coverage and premium of the cyberinsurance. Collaborative aspects are present between the insurers and the insured, as both want to keep the number of incidents as low as possible - the former, to minimize pay-outs, and the latter to protect their clients and business and maintain a good reputation. The advantages to collaboration are multiple: *(i)* businesses are gaining access to resources to fight lawsuits (lawyers), to provide advice about cybersecurity (cybersecurity experts) and other security competence. *(ii)* increased scrutiny related to cybersecurity can itself raise awareness and improve the overall security, especially for smaller organisations which might not have a large team dedicated to information and communication technology security [88].

Based on this characterization, cyberinsurance is included under the Identify function, as it deals with being prepared for issues once they arise, and hence can be seen as a governance issue. However, it can be argued, that the topic could belong also to the

Mitigation category of the *Respond* function, as it deals with containing the fallout after an attack.

[89] highlights the need for a global legal cybersecurity framework. In particular, the author finds that legal discussion on fighting against global cyber threats often emphasize international cybercrime and the application of warfare in the cyberspace.The author argues that the cybersecurity discussion should be extended beyond cyberwarfare. International collaboration on cybersecurity can help multinational organisations as they create a more coherent legal framework - a multitude of different international security rules, which vary from country to country can get difficult to navigate for organisations and can increase the potential for vulnerabilities - in countries with less stringent rules.

The paper cites four areas of focus for international cybersecurity law: *(i)* cybersecurity laws should be modernised, *(ii)* legal requirements should be uniformised *(iii)* more coordination should exist in regard to cooperative incentives and strong regulations and *(iv)* improvements to supply chain security should be made. In the context of this thesis, points *(iii)* and *(iv)* are more relevant and are discussed below. The author emphasizes the importance of cybersecurity to deter attacks and distinguishes between two types of deterrence.

Deterrence by punishment - refers to the threat that great harm will be inflicted on the opponent when unwanted behaviour happens, and *deterrence by denial* - refers to convincing an opponent to not pursue an attack, as its goals will not be attained without unreasonable costs [91]. Though deterrence by punishment is a useful tool for governments, it is deterrence through denial that can be helped by collaboration between the public and private sector. Moreover, cybersecurity is an area where the two sectors have aligned goals. Neither a rational executive nor a rational government official wants a company to experience cyberattacks. The author welcomes the progress made by various government bodies in the E.U. and U.S.A. to improve cyberthreat information sharing and proposes a better cybersecurity education and government tax credits or R&D funding to encourage research in cybersecurity. As the paper aims to improve the legal framework for organisations it can impact the regulatory environment in which it operates, and influences its governance, it was included in the Identify function section.

5.2.2 Protect

As discussed previously, (*cf.*, Chapter 2), collaboration requires people to work in a group and perform their allocated tasks and obligations. The parties involved in collaboration must establish common goals, divide and distribute the tasks among them and integrate the completed subtasks to complete the work. Based on the type of interaction between collaborators, [92] identifies a number of categories *(i)* Natural collaboration, *(ii)* Computer-Supported Cooperative Work, *(iii)* Human-Computer Interaction, *(iv)* A distributed system and *(v)* Robot collaboration. *Human-Computer Interaction* investigates how to improve collaboration between humans and computers by discovering more comfortable ways for human users to use computers. One of the challenges of this type of collaboration is to understand how humans naturally interact with each other and make the computers or machines more humanised. *Robot collaboration* is a newer topic of research which developed as robot technologies have evolved. Its goal is to team up robots with humans to complete tasks that a single robot could not complete. Once robots with human-like abilities will be developed, robot teams will be formed to accomplish complex tasks. A challenge of robot collaborations is ensuring that the necessary abilities for collaboration are possessed by the robots - this includes making decisions autonomously, avoiding obstacles and sensing each others.

Humans and collaborative robots (cobots)[1] work in close together to accomplish tasks. [94] propose a continuous user authentication method based on a biometric approach. The authors investigate how internal sensor data from cobots can be used to identify users by observing their physical interaction with the cobot to save an authentication template for the specific user. As most cobots have integrated sensors, the solution does not require for additional potentially intrusive hardware. The approach is based on machine learning and involves three phases. *(i)* The *training phase* involves obtaining information from the cobot sensors and extracting features to be used in user authentication - force and torque features proved to be most informative. *(ii)* In the *testing phase* interactions between humans and robots were compared to user profiles discovered in the training phase. Probabilities were assigned to actual interactions versus stored profile, and the highest probability was used to identify the user and update the current user's trust value. *(iii)* Finally, in the *continuous phase* the trust value was continuously monitored to determine if the user was allowed to continue working with the cobot.

As a continuation of the work, by the same author, [95] investigates further how the safety and security issues raised by the close collaboration between humans and robots can be tackled. Human-computer interaction is increasingly important with the increase in automation - especially in manufacturing, where human abilities are augmented by robots to increase performance and flexibility [95]. The solution proposed consists of a continuous form of authentication using wearable sensors - for instance an e-glove which tracks how users interact while performing their tasks. Using ML, dynamic behaviour feature vectors were mapped to users to ensure that only authorized users interact with certain exoskeletons or teleoperating remote robots. [95] believe this authentication method can serve well in other industries as well, such as in nuclear, space or offshore operations, but also in the healthcare field.

Further work on the topic of human-robot interaction was done by Gleirscher at al. [93], who investigate approaches and best-practices for safety and security of collaborative robots. The paper interestingly differentiates between various types of human-robot interactions, the two types on which the paper focuses, and which are also most relevant in the context of this thesis are (1) *cooperation* meaning humans and robots have shared work areas but do not simultaneously operate in the shared area; and (2) *collaboration* referring to humans and robots having shared work areas where they simultaneously, and potentially closely interact [93]. This distinction is consistent with the definition proposed previously (*cf.*, Subsection 2.2.1).

Introducing types of attacks identified by Trend Micro [96] - and presented in Table 5.2,

[1] Cobots refer to robots, including their operational infrastructure and software, intended for human and robot interaction and collaboration [93]

the authors discuss existing security approaches. Firstly *Security Policies* should exist, secondly *Authentication* is discussed. Approaches consist of passwords, tokens for users, or as proposed in [95], physical or behavioural features of users can be used for authentication. The authors also note that in most cases user authentication is one off, in contrast to the proposal by Almohamade et al. emphasizing the usefulness of the solution discussed above. Finally, *Intrusion Detection Systems* are discussed. The paper concludes with challenges to cobot security - the challenges identified are (1) developing security policies, (2) developing templates for authentication requirements, (3) developing strategies for cobot forensics and (4) developing IDS for use in collaborative robot environments.

Table 5.2: Summary of robot-specific attacks and their effects [96]

Attack Class and Description	Concrete Effects	Requirements Violated
Attack 1: Altering the Control-Loop Parameters - The attacker alters the control system so the robot moves unexpectedly or inaccurately	Defective or modified products	Safety Integrity Accuracy
Attack 2: Tampering with Calibration Parameters - The attacker changes the calibration to make the robot move unexpectedly or inaccurately	Robot damages	Safety Integrity Accuracy
Attack 3: Tampering with the Production Logic - The attacker manipulates the program executed by the robot to stealthily introduce a flaw into the workpiece	Defective or modified products	Safety Integrity Accuracy
Attack 4: Altering the User-Perceived Robot State - The attacker manipulates the status information so the operator is not aware of the true status of the robot	Operator injuries	Safety
Attack 5: Altering the Robot State - The attacker manipulates the true robot status so the operator loses control or can get injured	Operator injuries	Safety

Intelligent vehicles are becoming more popular, but attacks in their communication network threaten their security. Man-in-the-middle attacks and eavesdropping could lead to the collapse of vehicular network localization for cooperative location-sensing systems [97]. Z.Wang et al. propose a federated cryptosystem localization scheme. First, a federated localization scheme is designed, preserving privacy. Additionally, against eavesdropping attacks, Paillier[2] cryptosystem was combined with the localization scheme. The results show that secure location sensing can be achieved without adding significant amount of computational complexity and communication overhead in the context of cooperative location-sensing systems [97].

A different take on intelligent vehicles is proposed in [99]. Tang et al. highlight the risk of serious traffic accidents and crashes derived from hackers using vulnerabilities to

[2] The Paillier cryptosystem is a partial homomorphic encryption scheme - allowing users to perform operations on data that is encrypted without the need to decrypt it first [16], [98]

attack vehicles. Because single-point protection and lack of cooperation lead to insufficient protection for the Internet of Vehicles (IoV), the authors propose federated learning for IoV. ”Simple” machine learning trains models on a single machine, and distributed learning collects and allocates data, leading to transmission delay. Federated learning combines data from various clients to jointly train one common model. This is done without sharing the data, hence protecting user privacy.

The technique used consists of a three-layer neural network model which is trained on distributed equipment, and the training is performed by a stochastic gradient descent server. The findings show that the model has a high accuracy rate for attack prediction and can therefore be used by decision makers to develop measures to avoid potential attacks [99]. The aim of the paper, to use federated learning algorithms for predicting attacks. The prediction is performed before an attack happens; hence this work should not be included in the Detect section, therefore, it is included in the Protective Technology Category.

A serious threat to organisations is data exfiltration. A method to avoid exfiltration is perimeter defence, however, this is not offering sufficient protection, as exploits can be perpetuated by insiders too [100]. User activities on the internal network must therefore be monitored as well. On one hand automatic machine learning methods can be used to detect anomalies, however, these can create false alarms. On the other hand, domain experts can identify malicious users more precisely, but they have limited capacities to process large volume of information.

Therefore, M.H.Chung et al. propose interactive machine learning as an alternative, building a successful collaboration between machine learning algorithms and domain experts. The authors propose an active learning (AL) model where domain experts interact with the ML model - in particular, when interaction is adequate, domain experts can make quick adjustments to the model. The results show that AL can learn from anomaly detection outputs to prune false alarms. The conclusion reached is that the proposed interactive machine learning framework can work well in cooperation with domain experts who identify malicious attempts. Despite the emphasis on detection of the paper, it was included in the Protect category of the framework because of its forward-looking aspect and its emphasis on how to *prepare* for human and machine interaction.

One way to tackle the cybersecurity goal of confidentiality (*cf.*, Subsection 2.1.2) is by data anonymization. [101] investigate collaborative data anonymization with sensitive quasi-identifiers. This is useful in cases where respondents, because of privacy concerns, are not willing to reveal their full information to third parties. Collaborative anonymization refers to a group of respondents who anonymize their data collaboratively under a distributed setting - in the work of Wong et al. the approach taken is respondents collaborating with an agency to output jointly anonymized microdata. Quasi-identifiers (QIDs) refer to data that is not a unique identifier, but if used with external knowledge, or other QIDs, can lead to unique identification.

In contrast to other work, the authors propose a protocol for collaborative data anonymization that does not reveal the complete set of QIDs to the agency (data collector) as these can be sensitive and identifying values, meaning information that can be used to specifically identify individuals. The protocol, based on homomorphic encryption and

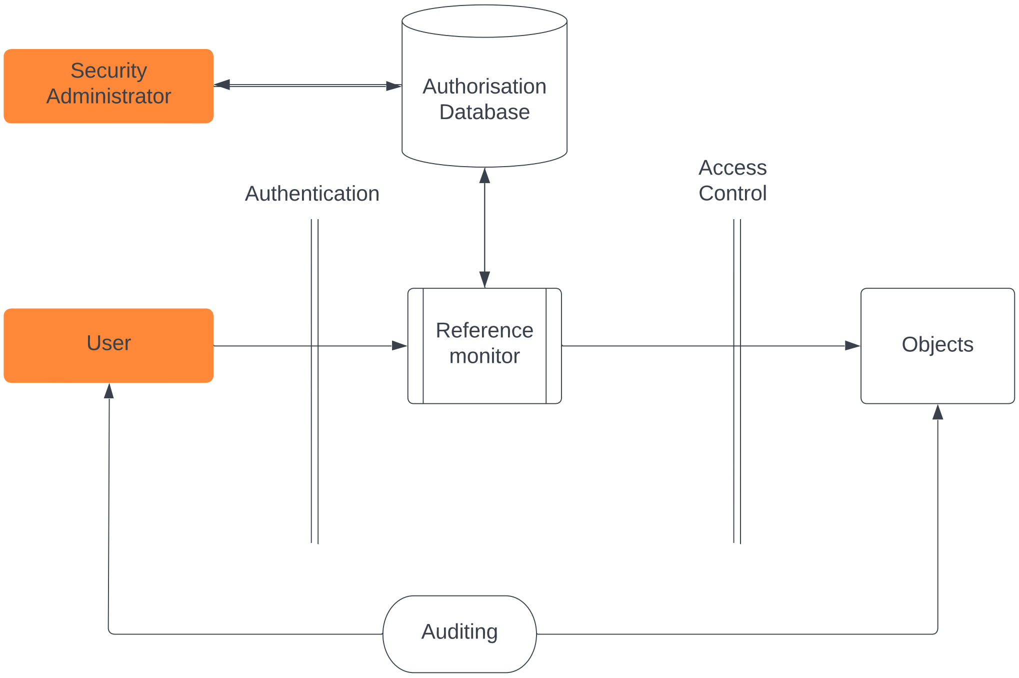


Figure 5.4: Access control and other security services [102]

respondent-agency communication through an anonymous public board, is also transparent, as respondents can verify if their information reached the agency unchanged and if the protection level guaranteed by the agency is reached before submitting the records. Finally, if an agency is malicious and makes invalid computations or modifies intermediate results, respondents can indict the agency.

These security features can alleviate the privacy concerns of participants. One aspect to be noted, however, is that the respondents can still submit inaccurate data, which can compromise the usefulness of the results obtained. The work by Wong et al. is included in the Information Protection Processes and Procedures as it deals with anonymization of data, which is a method to preserve the confidentiality of information - one of the main goals of cybersecurity.

The purpose of access control identified in [102] is to limit the operations and actions that a legitimate user can do to prevent activities that could lead to security breaches. Access control is enforced by a reference monitor(RM) which acts as a mediator for every access attempt by a user or by a program executing on behalf of a user. The RM consults a database with information about user authorisations which is maintained by a security administrator. The authorisations are set based on the security policy of the organisations. Finally auditing monitors keep a record of activities in the system. This relationship between security services is presented in Figure 5.4.

A different take on access control(AC) is proposed in [103]. In the context of public cloud storage services, data is outsourced outside the data owners' trusted domains, to semi-trusted cloud services. Encryption is often used to prevent access to sensitive data from

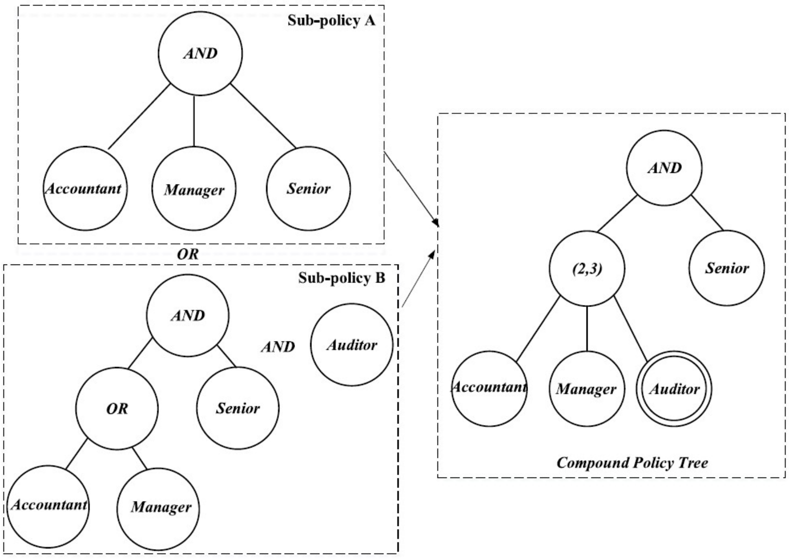


Figure 5.5: Access Policy Example [103]

the side of untrustworthy service providers. Attribute-based encryption(ABE) is a public-key authentication scheme where ciphertext can only be decrypted if a set of attributes of the ciphertext can be matched by the attributes of the user trying to access the data. ABE is collusion resistant - *i.e.*, no user key can be derived by collusion [104]. The authors claim that none of the existing ABE schemes support the use of collaboration for access permission - in existing ABE schemes, access permission is only assigned to individuals who own the attribute that satisfies the access policy.

Consequently, in [103] a special attribute-based access control scenario is explored, where multiple users collaborate to gain access permission while having differing attribute sets - as long as the data owner sets up the access policy in such way that collaboration is permitted. An important aspect to note is that collaboration not designated in the access policy is regarded as collision and access will be denied - in the context of an organisation where different teams work on different projects, this means that only users responsible for the same projects are allowed to collaborate and get data access in the scheme. The proposed access control scheme uses designated translation nodes in the access structure, enabling users to collaborate to satisfy a policy tree. The security analysis performed shows that the proposal supports controlled collaboration while data confidentiality is preserved, therefore providing fine-grained access control in environments where data must be accessed by multiple users that collaborate with each other.

Figure 5.5 illustrates the collaborative access policy. Data can be accessed by satisfying either sub-policy A or B. The former shows that individual users must satisfy the policy tree. The latter shows that alternatively the data can be accessed by collaboration on the condition that a user has access satisfying the left tree and a second one is an ”Auditor”. The two policies are expressed more efficiently in the compound policy tree, with the ”Auditor” node having two edges to show that it additionally allows collaboration to be performed on it [103].

[105] provide another insight into access control. Traditionally, AC has focused on using

a specific decision parameter to decide on access control - and usually these methods consider AC within a centralized administration. The Intranet of things, online social networks etc. constitute smart and collaborative computing systems (SCSs) to aid with the complex interactions among users, devices and organisations in order to administer activities and share resources among different participating entities, such as users, smart objects, cloud or edge computers.

The authors claim that SCSs require a different approach to AC, because of the multitude of users who can protect, manage, create and share resources in various ways, collaboratively or individually and even competitively. The paper proposes an activity control framework that is appropriate to the needs of a dynamic SCSs and a set of AC design principles for smart and collaborative computing systems. Rather than developing and implementing yet another access control model, the authors aim to define the scope of AC and develop its fundamental knowledge base in the context of smart and collaborative systems.

The principles proposed are explained based on a smart health use case. The example involves a doctor monitoring a diabetic patient who needs insulin when blood sugar level reach specific thresholds. The patient is wearing an insulin monitor and pump that can be turned on by the doctor remotely. Moreover, the patient can give family member or friends access to his data. The *Abstraction* principle refers to identifying the participants - by role(doctor), by relationship(family member), and by attribute(sugar, heart rate). The *Controllability* principle refers to the patient accessing her health data and access control - *i.e.*, give access to family members.

The *Containment* principle refers to minimising the damages users can make, in this case, the insulin pump not injecting more than a maximum dose daily. *Automation* refers to the automation of abstraction without action from the administrator - a doctor gaining specialized doctor role when a patient comes to see him/her for a special treatment. *Accountability* refers to holding participants and service providers accountable for their actions. Finally, *Searchability* refers to allowing a patient to search for a doctor. The paper discussed above only provides a framework and design principles, yet these are relevant for access control in a collaborative computing system, which is why the paper is included in the section on the Protect function under the Access Control category.

Finally, [106] approaches the topic of collaborative access control in the context of cloud storage systems. Existing implementations of cloud storage systems, for example HackMD or Google Drive are increasingly popular data storage and sharing and offer functionalities which allow multiple users to work on the same documents simultaneously.

The authors argue however that functionalities for collaborative access controls are lacking, preventing the wide adoption of cloud storage systems, especially in environments where system security and data privacy are of high concern. Current access control policies allow write or read accesses on an all-or-nothing basis, and do not allow for more specific controls, moreover, careless or intentional sabotage can be performed by single users, and there is no system in place to require multiple users to collaboratively control the access to critical files.

Table 5.3: Papers on the Protect Function

Work	Year	Category
[95]	2021	Access Control
[97]	2022	Protective Technology
[100]	2020	Protective Technology
[99]	2021	Protective Technology
[101]	2019	Information Protection Processes and Procedures
[93]	2022	Access Control
[103]	2019	Access Control
[105]	2021	Access Control
[106]	2018	Access Control
[94]	2020	Access Control

Therefore, [106] proposes a collaborative access control strategy based sets of users (called groups of managers in the context of the paper) allowing multiple groups to be connected and enhance the flexibility of the access control. The proposal consists of assigning n users as managers of a certain file, *f*. To get access to *f*, a certain number, m, of the n managers must agree to share their key with the requestor. It should be noted that the threshold, m, can differ for write and read request for the same file, and from file to file. Finally, in order to prevent single-point failures in the cloud storage, the files must be encrypted before being uploaded. An important distinction is also made between read and write accesses. The former can be decided based solely on the identity of the requestor, while the latter should in addition consider the nature of the modifications that shall be performed on the file. Modifications should be added to a log and the file should only be modified once a file arbiter, $u*$ audited them.

5.2.3 Detect

Information sharing can be defined as *"one-to-one exchanges of data between a sender and a receiver"* [107]. Information sharing can happen both on the side of the targets *i.e.*, defenders and in the camp of those who conduct cyberattacks *i.e.*, attackers. On the defenders side, three types of collaboration are distinguished, public-public, public-private and private-private, with the collaborators with the private side involved being the most cumbersome as privacy and civil liberty are not the only aspects to be considered - liability and economic costs have to be assessed too.

The information shared includes incidents - details about cyberattacks, vulnerabilities - exploitable weaknesses, and threats. However, the sharing of information might disclose critical information about the sharing organisation, hence defensive measures should be employed. These include *(i)Mitigation* taking precautions to prepare for future attacks *(ii)Situational awareness* assessing how to best handle an incident *(iii)Best practices*

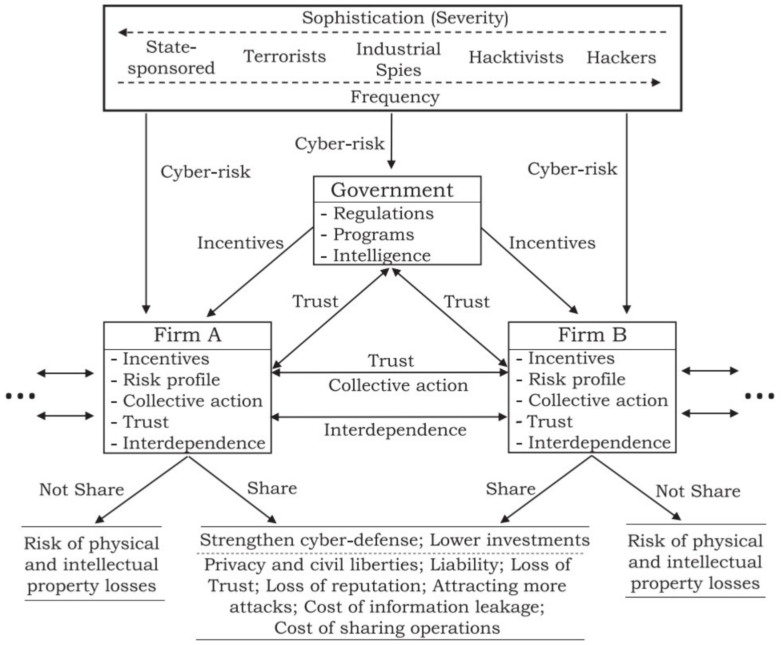


Figure 5.6: The Relations Between Actors, the Dynamics That Impact Collaboration Decisions, and the Cost–Benefit Aspect of Information Sharing from the Defenders' Perspective in the Face of Strategic Attackers from Different Sophistication Levels [107]

information on best actions in case of attacks and *(iv)Strategic analysis* using information to advance effective defensive measures.

Cybersecurity information-sharing (CIS) finds that coordination and cooperation help with mitigation and response in case of attacks [107]. Collective knowledge and capabilities are increased, and a better understanding of threats and risks is obtained. Moreover incentives for future attacks can be discovered and chances to detect attacks in the future are increased. Finally, CIS leads to reduced cybersecurity investments and aids at analysing future investment strategies.

There are however concerns about CIS, these include concerns about *privacy*, as CIS can lead to leaks of personal information being shared which can in turn lead to*loss of trust* of customers. This coupled with *loss of reputation* can have negative economic impact on organisations. Another serious concern is *inviting more attacks*, as malicious parties follow the news about defenders to collect information such as cyberdefence investment budgets, security-breach details in order to learn about opportunities to attack. Finally, CIS also comes with *costs of sharing operations* such as membership fees of information-sharing schemes, administrative expenses of labour, paperwork, and cybersecurity technological investments and updates [107].

Figure 5.6 provides a summary of relationships between the actors in CIS and how their collaboration functions. Attackers can threaten both governments and companies. The former develop laws and regulations to protect themselves and other organisations from attacks, encouraging firms to collaborate with the public sector and share information and vulnerabilities. Trust is also an important aspect that companies consider when deciding whether to share information both with other firms and with the government. When looking at private-private partnerships, firms forego investment costs thanks to stronger cybersecurity based on shared information, but they bear additional costs of sharing the information [107]

Open Data sources contain plenty of threat-related information, and early identification of emerging threats from this information is an essential part of security for systems and software [108]. Multiple methods for cybersecurity event detection that have been proposed to extract security events from text in open data sources - most of them with a focus on events which have many mentions, for instance on Twitter. While this is a useful way to gain awareness of attacks which impact numerous users, it might delay the response time.

A way to respond faster to attackers would involve stakeholders being aware of attacks as early as possible, regardless of how mentioned an event is [108]. A novel detection system which quickly identifies threats or attacks from Twitter regardless of the volume of mentions is proposed in [108]. The proposed method monitors new words and re-emerging words on Twitter, and identifies words related to security events. Clustering the tweets of well-known security experts linked by trigger words then helps narrow down candidate events among the hundreds mentioned. This approach leads to detection of new or resurgent security events without the need for a large volume of mentions on Twitter.

Similarly, [109] also investigates anomaly detection, but from large Cybersecurity Datasets. Arguing that this task is computationally expensive and challenging, the authors propose feature selection (FS) to select a subset of features, while removing the redundant or irrelevant ones. These can then improve the performance of machine learning algorithm performance.

[109] introduce a new anomaly detection approach - Anomaly Detection Using Feature Selection (ADUFS) to improve the scalability and accuracy of supervised and unsupervised ML techniques for anomaly detection. The proposed ADUFS involves an approach to select features based on cooperative co-evolution - an algorithm following a divide-and-conquer strategy to decompose large problems in a number of smaller sub-problems and optimize each sub-problem independently. These sub-problems are then combined to build a full solution to the main problem. The findings show that despite the time-consuming character of FS using evolutionary computation, if suitable FS processes can be identified before the anomaly detection, the detection performance can be significantly improved.

A more recent paper [110] looks at vulnerability disclosure on Twitter in the context of the COVID-19 pandemic. Arguing that the pandemic introduced a new way of working – working from home - which itself introduced new opportunities for hackers to attack through digital platforms. The usage of videoconferencing platforms, online shopping platforms, Virtual Private Networks (VPNs) increased the attack surface which could be exploited for launching cyberattacks. Existing research looks at Twitter for early identification of security events [108] or to explore vulnerability disclosure, however, there is a lack of investigation into opportunistic targeted attacks, where adversaries exploit vulnerabilities in a way that benefits them most in times such as during the COVID-19 pandemic.

[110] investigates the effectiveness of Twitter for vulnerability disclosure - specifically during COVID-19 and investigates how the social media platform can be used as Open-Source Intelligence during a pandemic. The study also uses Twitter to identify cybersecurity awareness campaigns. The findings show that Twitter was used by multiple stakeholders to disclose vulnerabilities (security researchers, ethical hackers, among more unlikely actors such as consultancy firms, and many more). The findings also highlight the difficulties of validating cybersecurity awareness campaigns, as they were dispersed and conducted by individuals, and raising concerns that misleading campaigns by individuals can be initiated along legitimate government sponsored ones.

[111] investigates the topic of vulnerability disclosures (VD) from yet another perspective. VD's purpose is to ensure that users address the vulnerabilities before malicious parties can find and exploit them - and [111] focuses on this dilemma of ”disclose or exploit”. It presents a ”two-player non-zero-sum simultaneous cyber-security game” [111] between a hacker and an organisation. The game is played for multiple rounds. The hacker can act separately, or collaborate with the organisation. In the next stage, the organisation is faced with the same choice, act independently, or collaborate with the hacker. The paper proposes an algorithm to determine the Nash equilibrium of the game.

The results of the study show that organisations can take an active approach when negotiating with grey hat hackers, and these will respond to the organisations move. This approach which implies that the hacker will become more transparent towards the organisation as such, the organisation will collaborate with him, which will result in a more effective solution than introducing legal action against the hacker. Of crucial importance is the timing of the game - the maximum cooperation occurs when the parties will decide to collaborate at the beginning of the game. When one of the two sides decides to extend the game or act independently, the benefits of collaboration are lost. The benefits of collaboration are that the hacker's decision to exploit vulnerabilities will be minimized, and the organisation will become aware of the vulnerabilities and create a safer environment.

A further look at data sharing is offered by [83]. As mentioned, despite being proposed as a great way to enhance cybersecurity, data sharing across organisations is a challenge for confidentiality, trust and liability. [83] Freudiger et al. investigate a *controlled data sharing* approach for collaborative threat mitigation. The authors argue that using cryptographic tools, organisations can estimate the benefits of data sharing. The authors focus on collaborative predictive blacklisting - forecasting sources of attacks based on the organisation's own logs as well as logs contributed by collaborators. The three focus areas are: *(i)* how to estimate the benefit of data sharing for organisations, *(ii)* how can the benefit estimation be performed in a privacy-preserving way and *(iii)* what and how much data should organisations share, once they have decided to collaborate.

The results successfully answer the 3 points outlined above. Firstly, as expected, the more information about the attackers is available, the better the prediction is - the prediction analysis investigated the correlation between the number of events known by targets and their ability to predict attacks. Secondly, some collaboration strategies yield better results than others, and the prediction accuracy heavily depends on the strategy employed, in the case of some strategies, the sharing is in fact not helpful at all. However, when a successful strategy is used, a better prediction is not the only improvement noticed -

additionally, the false positive rate is reduced. Finally, sharing only information about common attacks, is almost as useful as sharing all the information available, leading to the conclusion that controlled data sharing can indeed help organisations find the amount of data that is just enough to improve prediction [83].

This paper is complex to assign to a single NIST category - it deals with prediction of events, which is why it is included in the *Detect* section, however, it can be argued that it could be also added to the *Prevent* or *Recover* section, as other similar papers were. The decision was made based on the fact that the *Prevent* function does not have a specific category for predicting attacks, and the Recover function is focused on the communication rather than the actual prediction of events.

[112] distinguish between different concepts related to intrusion. Firstly, *intrusion* itself is defined as an attempt to compromise one of the confidentiality, integrity or availability or to bypass the security mechanisms of a network or computer. *Intrusion detection* refers to the process of monitoring the computer or network to identify unusual events and analyse them for any sign of intrusion. *Intrusion detection systems* are hardware or software systems aimed at automating the process of intrusion detection. Finally, *Intrusion prevention systems* have all the capabilities of intrusion detection systems but could also attempt to prevent incidents from happening.

Intrusion detection methodologies can be divided in three types. *Signature-based Detection* refers to the process of monitoring the network traffic to identify signatures or patterns corresponding to a known attack. It is the simplest and an effective method to detect known attacks, but it is inefficient for detecting attacks with unknown signatures and patterns, as well as variants of known attacks. This leads to the issue of having to permanently update the information on signatures or patterns of possible attacks which is time consuming [112].

Anomalies refer to deviations from known and expected behaviours, while profiles represent the expected behaviours. Therefore *Anomaly-based Detection* refers to comparing actual observed events to profiles to identify deviations and recognise attacks. This type of detection is effective at identifying new, unforeseen vulnerabilities and can help with the detection of privilege abuse of insider actors. However, drawbacks include weak profile accuracy due to changing behaviours, and unavailability during the building and rebuilding of behaviour profiles. Finally, it can be difficult to trigger alerts fast enough [112].

The third and final detection methodology is *Stateful protocol analysis (SPA)* which refers to an IDS that traces protocol states, for example pairing requests with replies. On a first look SPA seems similar to anomaly-based detection, however it distinguishes itself from the latter as it depends on generic profiles deployed by vendors, rather than preloaded network-specific profiles. It is useful to distinguish new and unexpected command sequences, however it is unable to identify attacks that seem benign protocol behaviours and might be incompatible to specific operating systems [112].

[113] details a number of various machine learning applications in cybersecurity. Of relevance for this topic of collaboration is the Vehicular ad hoc network (VANET), a fairly recent technology in transportation systems which aims to provide road safety and comfort to travellers while protecting the privacy of the driver. Intrusion detection systems

(IDSs) can be used to mitigate threats by detecting malicious behaviours or abnormal actions. Collaboration among vehicles in the VANET leads to a more accurate detection of anomalies, and distributed machine learning provides a good methodology for designing algorithms for collaborative detection over VANET. A problem with collaborative learning is the potential of compromised data as nodes exchange data between them. This risk can be mitigated by using a privacy-preserving mechanism [113] - able to provide a string guarantee of privacy.

A different area in which cybersecurity and cooperation are used for autonomous vehicles (AVs) relates to Cooperative Intelligent Transportation Systems (C-ITS) [114]. AVs are controlled by Autonomous Driving Systems and are outfitted with a number of sensors to receive information from their environment. As noted previously, vehicles can exchange real-time data among each other, which can lead to a reduced number of traffic accidents and reduced congestion, as well as improve the efficiency of the transportation systems. However, these constant interactions with their environment create a broad attack surface for AVs. The sensory data used is susceptible to anomalies with diverse causes: sensor malfunctions or faults, but also, malicious attacks.

The authors propose a collaborative anomaly detection methodology, Autonomous Driving Systems with Lifelong anomaly detection (ADS-Lead) in order to protect the mechanism that autonomous vehicles use for lane-following. The proposal introduces a transformer-based one-class classification model that helps identify time series anomalies in examples of adversarial images - detecting GPS spoofing, lane detection attacks and traffic sign recognition.

Moreover, the constituent vehicles of a C-ITS form a cognitive network on which federated learning can be applied so that the vehicles jointly update the detection model. The evaluation performed on Baidu's Apollo[3] shows that the proposed solution can effectively detect sensor anomalies and outperforms other state-of-the art anomaly detection models [114].

Systems-of-Systems (SoS) are collections of systems combining their capabilities and resources to accomplish specific goals that would not be achieved by single systems [115]. The SoS does not have control over the behaviour of each constituent system (CS), as each CS is operationally and managerially independent. The collaborative nature of System of Systems increases the risk of vulnerabilities which can be exploited by cyberattacks [115]. For example, attackers could try to impersonate individual CSs' or manipulate data from different CSs introducing vulnerabilities to SoS data privacy. Model-based testing to automatically generate test cases can lead to discovering vulnerabilities, however this process is time- and labour-intensive, as well as error-prone.

[115] propose an automated test data generation using a model-checking technique which generates counterexamples when the violation of certain security properties is detected. The results show the method proposed can turn counterexamples into test cases and generate concrete test data able to identify known vulnerabilities in the System of Systems. The authors find that modelling an adversarial as well as typical system, and generating

[3] https://apnews.com/article/technology-china-electric-vehicles-artificial-intelligence-aa40645d1aac6f8348d1208a659d6c25

test cases, can assist experts with the generation of executable tests that can then be used to test the security of the system [115].

Honeypots are computer systems whose aim is to serve as decoy in cyberattacks, as they can be purposely weakened to become more vulnerable than other systems and attract attacks [116]. Detecting ransomware attacks is challenging and resolving the attack, *i.e.*, gaining access back to the information or the systems, is particularly difficult because of the complexity of the encryption algorithms used. Once a device is infected, components and systems connected to the same network become vulnerable as well.

[116] propose a method to detect ransomware attacks and to prevent data loss using honeypots. The work features a file-based honeypot method - the basic idea being that synthetic files and folders are created to identify new types of malware, and use the information obtained from logs to develop new and precise security prevention mechanisms. The novelty of the proposal comes from the fact that a custom set of rules is applied for honeypot deployment - based on multiple symbolic links to a single honeypot, rather than controlling for numerous decoy files. The approach is tested, and a detection rate of 100 percent is reached for all the experiments, leading to the conclusion that ransomware can be effectively detected using file symbolic linking honeypots [116].

[117] also used a honeypot method and propose *Honeypot-To-Go (HosTaGe)* for mobile devices. The system has a user-centric design and can be run out-of-the-box on devices using the Android operating system. The solution was created in the context of an ever-growing number of free, open wireless networks. Users will connect to these ubiquitous networks without questioning their security reliability and overall worthiness. The large number of interconnected users, devices and networks can be used in two ways: *firstly* and unfortunately, the wireless networks can be used by malicious parties to attack - compromise or infect - the devices connected to the network. *Secondly* and more positively, the wireless networks and devices connected to them can be defended and simultaneously used to create a community of defenders which exchange alert information and collaborate to mend off attacks and reduce the attack surface.

[117] argue that in contrast to Intrusion Detection Systems of dynamic firewalls - which are passive methods to detect malicious behaviour, usually deployed on non-mobile devices, honeypots are a more active way to gain an in-depth view at the activities of the malicious parties. In particular, low-interaction honeypots, which are used for the proposed solution, are suited for mobile devices. The *HosTaGe* alerts users about the security health of the wireless network they are connecting or connected to. It can detect malicious activities and network misconfiguration and is a community-based initiative, as it collaboratively exchanges alerts among other instances of the *HosTaGe*. The result of the utilization of the proposed solution is firstly that users will be encouraged to be more mindful and cautious when connecting to open wireless networks, and secondly, that malware propagation will be reduced [117].

A sophisticated attacker can spend 100 days or even more in a system before being detected, even with advanced monitoring in place [90]. The authors propose a collaborative framework that aims to provide assistance to security analysis by using semantically rich knowledge representation and reasoning combined with various ML techniques to detect cybersecurity attacks and anomalies. The mechanism used works as follows, it draws information from different text sources, such as blogs, security bulletins etc. and then combines the information and stores it into a knowledge graph using terms from the Unified Cyber Ontology network[4].

The represented data comes from network sensors and from traditional hosts in the same graph. Subsequently, it searches through this knowledge to detect events relevant to cybersecurity and to predict potential attacks. The developed proof of concept technique reduces the effort on cybersecurity analysts - combining information from multiple sources and reasoning over it in the context of cybersecurity events in large organisations [90].

A number of machine learning approaches has been identified so far in this chapter, showing their importance in fighting cyberattacks. [119] argues that to be able to implement successful ML algorithms in the industrial Internet of Things (IIoT) it is necessary to develop new computing approaches to avoid the increasing costs associated with the instalment of new state-of-the-art edge[5] analytic devices [119].

The author proposes a collaborative computing method to construct a Gaussian Mixture Model, a clustering technique that uses Gaussian distributions. The parameters for the GMM are learned in the cloud, but the actual GMMs are constructed at the edge layers. The method proposed in [119] creates the possibility to shift certain complex applications, such as ML based cybersecurity applications, to the edges of IoT networks while using inexpensive, widely available digital signal processors.

The rise in intelligent devices and the ubiquitous connectivity associated with them has increased the Internet of Things (IoT) traffic in the cloud environment dramatically, creating the potential attack surfaces for cyberattacks [120]. As the authors find that the traditional security approaches are insufficient to protect the cloud-based IoT networks, they propose an intelligent collaborative network-based intrusion detection system (NIDS) for software defined networking (SDN)[6] based cloud IoT networks. The proposal is composed of a hierarchical layer of intrusion detection system nodes that collaborate to detect anomalies and instruct the SDN-based gateways devices to halt malignant traffic as soon as possible [120].

Similarly, another work [123] covering SDNs but this time in the context of Service Function Chaining(SFC) *i.e.*, a capability using SDNs to create a chain of connected network services such as intrusion protection [124]. The authors create a collaborative Security as a Service system by using the SFC's ability to manage security service functions - are a type of on-path service function which detect and mitigate security threats, for example a firewall for filtering traffic. [123].

A different take on intrusion detection (ID) is proposed in [125]. Here, an adaptive collaborative ID method aimed at improving network safety is introduced. The proposed

[4] The Unified Cyber Ontology is a community developed model aimed to provide a foundation for standardized representation of information across the cybersecurity world [118]

[5] Edge devices are devices that serve as an entry point into the core networks of organisations or service providers

[6] Is an architecture aimed at increasing the flexibility of a network and increase its ease of management by enabling intelligent and central control of the network [121], [122]

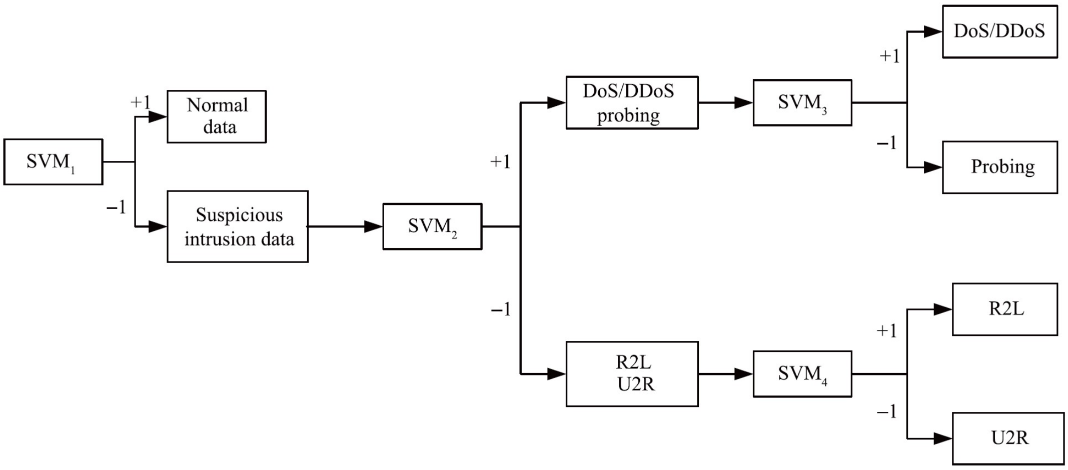


Figure 5.7: Collaborative intrusion detector based on SVMs and DT for TCP proposed in [125]

model is based on 2-class support vector machines (SVM) and decision trees (DTs) [7] and applies the Environments-classes, agents, roles, groups, and objects (E-CARGO) model to help design the detection system. The paper focuses specifically on Transmission Control Protocols, which help exchange messages between the devices connected to the network and detectors.

The adaptive, collaborative ID model is implemented as shown in Figure 5.7 - first the data is separated in normal and suspicious, at the second layer the SVM separates the intrusion data into DoS or DDoS and probing attacks, and remote-to-local (R2L) and user-to-root (U2R) attacks. Finally, in the last layer, the individual attack types are detected. The effectiveness of the proposed model is evaluated, and the results show that the model is more accurate compares to detector systems with single type SVMs [125].

The following paper [128] discussed intelligent software agents for operation and response in the context of power grids. The agents are applications connected through a network and can be vulnerable to cyberattacks. The authors therefore aim to prevent attacks and reduce the consequences of attacks that were successful. The architecture introduced contains multiple layers of verifiable, small agents which communicate and collaborate with each other to share data about the state of the power grid.

Moreover, the agents also collaborate in utilizing strategies to limit the effects of an attack. *(i) Communication agents* receive data from external sources, the data is validated, the spoof messages are discarded, and it is exchanged with the *(ii)distribution/voting agent(DVA)*. Here the data is validated again and communicated further to the *(iii) replicated computational agents(RCA)* where the data is processed. Each RCA sends the processed information individually to the DVA. If the RCA is compromised - it does not respond, responds slowly or incorrectly - the *(iv) monitor/resurrection agent* replaces the corrupt RCA with a new agent. Finally, the *(v)mutation agent* will update and execute source code to prevent successful attacks to be repeated.

[7] Both Support Vector Machines and Decision Trees are supervised learning models used for classification [126], [127]

Table 5.4: Papers on the Detect Function

Work	Year	Category	Secondary Category
[108]	2020	Anomalies and Events	R - Communication
[109]	2022	Anomalies and Events	-
[110]	2021	Anomalies and Events	R - Communication
[113]	2018	Detection Processes	-
[111]	2022	Security Continuous Monitoring	-
[123]	2018	Detection Processes	D - Anomalies and Events
[115]	2022	Anomalies and Events	-
[116]	2021	Anomalies and Events	-
[90]	2018	Anomalies and Events	-
[119]	2018	Security Continuous Monitoring	-
[120]	2019	Anomalies and Events	-
[114]	2022	Anomalies and Events	-
[117]	2014	Anomalies and Events	-
[83]	2015	Detection Processes	RE - Communications
[125]	2017	Anomalies and Events	-
[128]	2007	Security Continuous Monitoring	-
[129]	2019	Anomalies and Events	RE - Communication
[130]	2014	Anomalies and Events	-

The proposed multilevel agent architecture builds on collaboration and communication between various agents. Because it discusses continuous monitoring of the network to identify and prevent attacks, the paper is included in the Detect function section under continuous network monitoring.

Interest is increasing in cyber threat intelligence (CTI) as it can serve as a defence for advanced persistent threats (APTs). A key component of CTI is sharing of threat information among a number of collaborators. A manual time-consuming process for a long time, threat information sharing has been investigated recently and a focus on automation standards exists now. The standards are aimed at converting the information on threats into standardized, machine-readable data. The focus in [129] is creating a scalable real-time information sharing system for the cloud, drawing upon current achievements of private companies and researchers. The authors hope that the excessive amount of various standards and platforms for threat information sharing will find a way to cooperate or restructuring their methods to be compatible with each other.

Monitoring cyberattacks before they are launched is not possible, however threats can be analysed to be better protected. As discussed previously (*cf.*, Subsection 2.1.4) threats are exploiting vulnerabilities to impact a network or an information system. The authors identify two types of threats *(i)* low-level which refer to software and system vulnerabilities, and *(ii)* high-level, related to ATPs. Organisations are consuming threat information - containing attacker identification, attack approaches, targets and vulnerabilities of targeted systems, as well as details about previous attacks and potential solutions - received from CTI to obtain on understanding of attacker's behaviour in the context of APTs.

The authors propose a framework of scalable real-time threat information system in the cloud based on five units. *(i)* The *Trust evaluation unit* maintains a watch list containing the trust scores of collaborators to evaluate their trustworthiness. The trust score is judged on factors such as the quality of the submitted threat information feeds. *(ii)* The *Threat data collection unit* gathers data from collaborator submitted structured threat information feeds and raw data feeds from heterogenous sources. *(iii)* The *Centralised analytics unit* pre-processes and analyses the threat data and generates an interpretation and investigation of the threat information *(iv)* The *Storage unit* maintains a searchable storage of the standardised threat information feeds that were generated and caches the data collected. Finally, *(v)* the *Integration unit* related to the distribution and sharing of the threat information, and the integration of information feeds among collaborators.

The authors note that it is important to choose the most valuable threat information feeds for integration, taking into consideration cost, latency and defensive outcome *i.e.*, collaborators might miss vital information from uncommon feeds if they focus on the most popular ones. Threat information sharing is inherently collaborative, this paper focus on identifying vulnerabilities and sharing them across collaborator, warrants its inclusion under the Detect function.

Cloud computing provides a model of flexible network computing allowing organisations to adapt their IT capabilities to their needs fast and with little investment in IT [130]. However, there are also drawbacks to cloud computing, as security vulnerabilities are inherited from the underlying technologies used. These are preventing organisations to adopt cloud computing for numerous critical business applications as they leave loopholes that can be exploited by malicious parties. The authors of [130] are arguing that to guarantee security multiple security schemes - such as authentication, access control, encryption, IDSs, data leak prevention systems (DLPSs) - must be used collaboratively.

IDSs are sensing attacks in computing systems and alerting the users, therefore they provide a level of protection against malicious users. They can be classified in *(i) Host-based IDS (HIDS)* which are detecting malicious events on host machines and handling attacks such as insider attacks and user-to-root attacks. *(ii)Network-based IDS (NIDS)* are monitoring and flagging traffic that transports malicious content handling attacks such as port-scanning and flooding attacks. Because the cloud computing model has multiple entry points it is vulnerable to cooperative intrusion - attackers can try to penetrate the network through all entry points, and as behaviour at each point is not different from the normal, it can evade traditional IDS. The authors are proposing a collaborative intrusion detection framework to improve the security of cloud computing systems. NIDS and HIDS cooperate to carry out intrusion detection both at network and host levels each IDS having both anomaly- and signature-based detectors. The framework is comprised of *(i) Cooperative agents* who are installed either on host machines and equipped with HIDSs or on monitor the network and are equipped with NIDSs and a*(ii)central coordinator* which performs an aggregation of network traffic which enables it to capture sophisticated cooperative attacks.

5.2.4 Respond

As the amount of cyberattacks as well as their sophistication increase, cooperation by sharing of information is a promising strategy to mitigate this issue [131]. Organisations will search for a win-win situation in regard to sharing and therefore need to be incentivized to do it.

[131] presents a model to investigate the advantages and disadvantages of information sharing across organisations with some dependencies. The model uses functional dependency network analysis to imitate attacks propagation and game theory for the management of information sharing. The model was tested in a particular scenario - with the results pointing to an improvement of the general welfare by information sharing. The model can be used to try to find beneficial sharing policies. This approach can improve the response during cyberattacks beyond individual organisations, as external stakeholders can be involved and prevented of attacks as well.

[70]applied an agile incident response (IR) framework to processes in healthcare. Traditional incident frameworks are linear in nature and include similar stages with the NIST cybersecurity framework: prevent, detect, contain, eradicate and learn. The study by Y.He based on the Agile Manifesto proposes a new agile framework to improve the linear IR processes. Using the IR framework of Britain's National Health Service(NHS) the authors show how this can be adapted into an agile framework.

Based on this description, the study actually covers all steps of the NIST Framework. The decision to be included in the *Respond* section of this paper is based on the fact that the Response Planning subsection is concerned with response processes and procedures being maintained and executed in case of attacks. As such, this framework can be seen as a procedure in the event of an attack and can be classified as a response planning solution. The authors find the Agile principles can be combined with a linear IR framework or a fully Agile framework can be created. Both options aim to aid with a quick reaction from attacked organisations to bring them back to a business-as-usual state as soon as possible. These alternative frameworks are more fitting for a breach that happens in real life "unexpected, fast spreading, and multi-faceted" [70] and which does not necessarily follow the archetypical IR steps.

Traditional network worms are a type of malware that features some degree of intelligence and automation. They are able to infiltrate the computer network and attack node hosts that display vulnerabilities [132]. In contrast, benign worms can defend the computer network through replication and propagation. As an example, if host X knows that host Y has a vulnerability, X it can transfer benign worm defence code to Y in order to correct the vulnerability, or to defend against an attack. [132] propose the concepts of worm computing and worm nodes - in this computing model, information from the internet is integrated by worm nodes to provide collaborative defence. Secondly, it proposes a blockchain technology where the distributed architecture for worm computing can be

Table 5.5: Literature classification based on function

Governance	Identifying attacks	Protective Measures
[73] 2017	[108] 2020	[95] 2020
[74] 2017	[109] 2020	[94] 2021
[77] 2022	[110] 2021	[93] 2022
[76] 2020	[111] 2022	[100] 2020
[72] 2022	[83] 2015	[99] 2021
[78] 2021	[114] 2022	[101] 2019
[79] 2020	[116] 2021	[105] 2021
[80] 2020	[117] 2014	[106] 2018
[81] 2013	[90] 2018	[133] 2018
[86] 2020	[119] 2018	[97] 2019
[87] 2021	[120] 2019	[103] 2019
[82] 2012	[125] 2017	[131] 2016
[88] 2015	[123] 2017	[132] 2021
[89] 2018	[134] 2018	[135] 2020
[70] 2022	[115] 2022	
[71] 2019	[113] 2019	
[136] 2018	[137] 2019	
[138] 2021	[128] 2007	
[84] 2019	[129] 2019	
[37] 2022	[130] 2014	

constructed, and finally it analyses the implementation strategies for the proposed model and assess its effectiveness. The findings show that the proposed model involving worm computing is successful in improving resource utilization and cybersecurity.

[71] investigate factors related to the development of a culture of cybersecurity at an organisational level, as well as the communication and cooperation struggles faced by a computer security incident response team (CSIRT). The findings identified a number of obstacles in the smooth running of CSIRT teams. Most important are obstacles related to coordination and communication - the issues can occur on two different levels. between employees and management, and between employees in a team. Additional obstacles identified are expressed in Figure 5.8. Recommendations include managers investing in the creation of a culture of collaboration visible to everyone in the team, as well as provide trainings for collaborative behaviour. Finally, an important aspect is that teams should consist of a mixture of new and more seasoned employees.

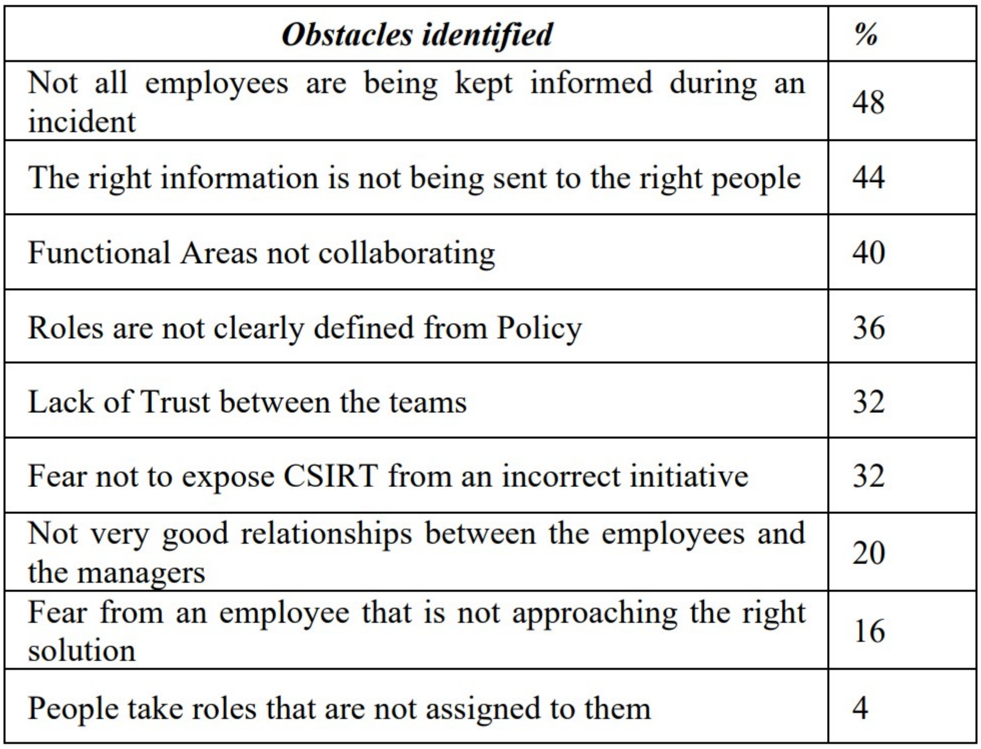
The interaction between ML models and domain experts is explored in the Protect Subsection (*cf.*, 5.2.2) where [100] proposes interactive ML where algorithms and domain experts collaborate to avoid data exfiltration. On a similar note, [134] learn from experts' experience to execute cybersecurity data triage. Cybersecurity operations centres (SOCs) use a number of methods to measure network events. The collected data must be investigated by human analysts in order to reach conclusions on incident detection and response. The sheer amount of information collected is often overwhelming for analysts and the time demands of the triage, leave little opportunity for the in-depth analysis of information needed for producing qualitative incident reports in a timely manner.

[134] propose data triage automatons to reduce the workloads of analysts. Data triage refers to the process of analysing the details from a variety of data sources - firewall logs, intrusion detection system alerts etc. - to exclude false positives and to group together indicators that are related so that a separation of different attack plots is performed. The authors constructed a human-in-the-loop case study where thirty professional analysts completed cyberanalysis and their operations were recorded. Their process was then used to construct finite state machines in order to automate the data triage.

The results, comparing the automated data triage with the cybersecurity experts' triage, showed that conducting automated data triage by using the analysts' traces is feasible. The automatons were able to process large amounts of data more time-efficiently and a satisfactory false positive rate was achieved - the false negative rate still needs improvements. An interesting result is that selecting traces from analysts' which have a better task performance also improves the performance of the automated triage system. The paper is included in the Response planning system, as analysts in SOCs often need to conduct multiple analysis, including threat and forensic analysis and *incident response* [134].

Software Defined Networks were previously discussed and implemented in the context of the Protect function of the NIST framework. In [133] SDN is combined with Moving Target Defence (MTD). DDoS attacks targeting the availability of network and computing resources are a serious threat to organisations - to limit the negative effects caused by distributed large-scale cyberattacks, a collaborative and scalable mitigation approach, combining MTD and SDN is proposed by the authors. Cybersystems often have a static configuration - this is an advantage for attackers, as they can perform reconnaissance to determine potential vulnerabilities and choose the best way to attack.

An alternative to static configurations is MTD - a concept of controlling change across multiple system dimensions to increase the apparent complexity and uncertainty in the face of attackers, therefore making the discovery of vulnerabilities and development of an attack plan more difficult [139]. The solution proposed by the authors brings a number of contributions: *(i)* aims to limit the impact of DDoS attacks in high-speed networks by combining MTD and SDN and *(ii)* the collaborative defence solution has a low cost and can be integrated into existing infrastructure. [133] show that the probability of successful DDoS attacks decreased with an increase in collaborative partners processing the network traffic and using MTD. Moreover, the MTD strategy significantly reduces the effects of large-scale cyberattacks. The final point represents the reason why this paper, despite investigating a defence mechanism is included in the Mitigation Section of the Response stage.



Obstacles identified	***%***
Not all employees are being kept informed during an incident	48
The right information is not being sent to the right people	44
Functional Areas not collaborating	40
Roles are not clearly defined from Policy	36
Lack of Trust between the teams	32
Fear not to expose CSIRT from an incorrect initiative	32
Not very good relationships between the employees and the managers	20
Fear from an employee that is not approaching the right solution	16
People take roles that are not assigned to them	4

Figure 5.8: Obstacles in communication/coordination during an incident [71]

[135] discuss predicting cyberattacks in a collaborative environment. More specifically, they propose to exchange ID alerts across organisations and networks rather than trying to predict attacks by focusing on single observation points, as it is very difficult to provide all the information needed for detecting an ongoing network attack and predicting the next event by using a single observation point. The paper follows three levels of cyber situational awareness - the application of the concept of situational awareness to cybersecurity[8] - perception, comprehension and projection.

Regarding *perception*, the authors investigated how alerts from various heterogeneous sources could highlight interesting features, such as whether events are isolated or related to larger events. When it comes to *comprehension*, the authors show how data can be understood and interesting patterns can be extracted by using data mining and alert correlation - an interesting finding was that 85% of security alerts are duplicates. Rule mining and sequential pattern extraction methods were introduced to find models of attackers' activities. Finally, the stability of the results across days and weeks, permits the use of predictive analysis over alerts, and represents the third situational awareness stage - *projection.*

[8] Situational awareness is defined as the ”Perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future [135]

Table 5.6: Papers on the Respond Function

Work	Year	Category	Secondary Category
[131]	2016	Communicate	DE - Anomalies and Events
[70]	2022	Response Planning	ID, PR, DE, RC
[132]	2021	Mitigation	-
[71]	2019	Improvements	RE - Response Planning
[134]	2018	Response Planning	DE - Anomalies and Events
[133]	2018	Mitigation	DE - Anomalies and Events
[135]	2020	Mitigation	

5.2.5 Recover

As the risk of cyber incidents rises, users of the internet, governments, organisations are all faced with damage to computer systems or data theft. The U.S. federal government considers information sharing on cybersecurity issues of utmost importance [136]. Therefore, it has created the Information Sharing and Analysis Center (ISAC) to encourage the trusted information exchange between both the public and the private sector, as well with individuals. The authors illustrate a number of information sharing structures between the government, ISAC and other participating entities while discussing strategic interactions between a number of stakeholders. This information sharing can be an important step in the *Recovery* step after a cyberattack, as it can serve as a lesson for other stakeholders. Figure 5.9 shows fifteen information sharing structures, these range from a simple interaction between the government and an entity *(a)* and more complex structures such as *(n)* where an entity is not aware of specific attacks directed against itself but wishes to be aware of trends and indicators. In this case ISAC would give an overview of relevant information to its constituencies.

Electrical grids are regarded as one of the most critical infrastructures in a number of countries [138]. Consequently, a large amount of literature is dedicated to the vulnerabilities and security properties of the technologies used in the electrical power industry, but there is little literature about the interactions across organisations that operate in the U.S. electrical power industry, particularly relating to the communication and collaboration in case of cybersecurity threats.

The exploratory qualitative study of [138] investigates the sharing of information among cybersecurity professionals involved in the U.S. electrical grid - this is done through interviews with 13 participants from 10 organisations involved in the U.S. electrical power industry. It is worth noting that communication is an aspect involved in all NIST stages to some extent, and particularly in the *Recover* and *Respond* ones, where these are defined as individual subsections. As such, it is difficult to say with absolute certainty where this paper should be included. The decision to add it to the *Recover* section is based on the fact that the main research question of [138] relates to information sources used by cybersecurity professionals in the electrical grid industry to ”share information

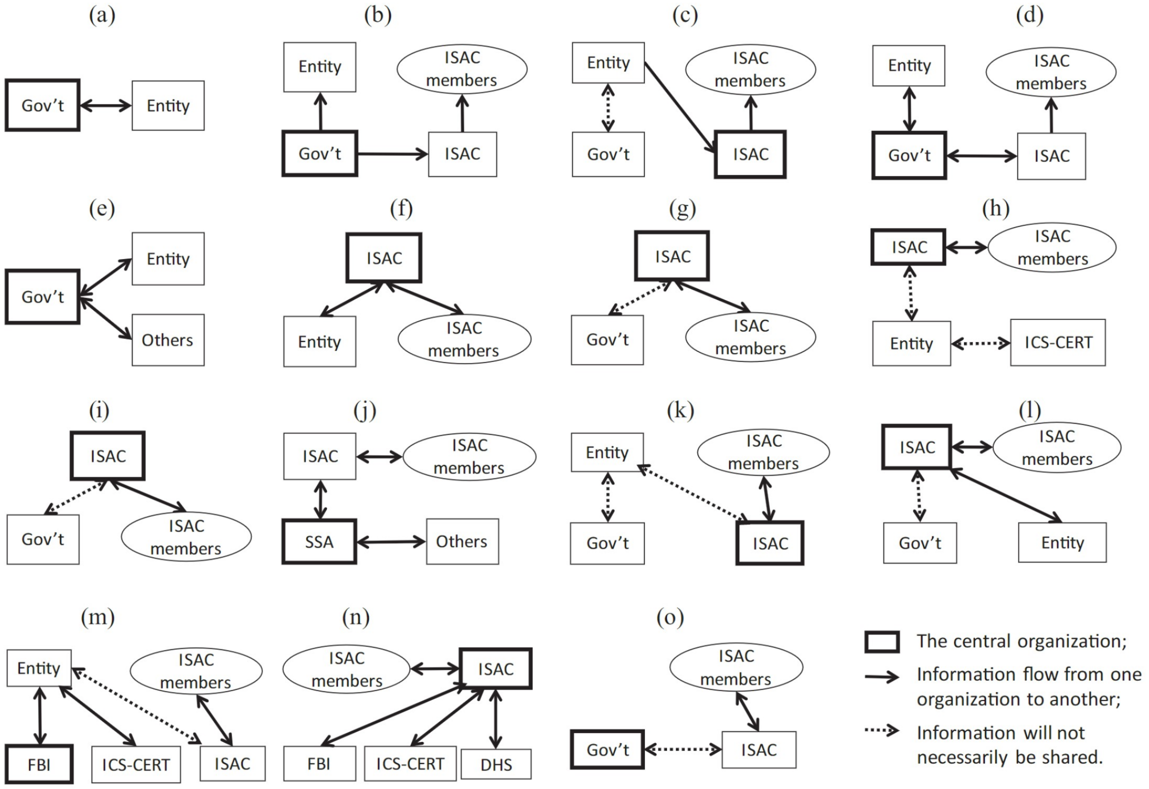


Figure 5.9: Fifteen representative information sharing structures [136]. ISAC = Information Sharing and Analysis Center, ICS-CERT = Industrial Control Systems Cyber Emergency Response Team, SSA = Sector-Specific Agency, FBI = Federal Bureau of Investigation, DHS = U.S. Department of Homeland Security

Table 5.7: Papers on the Respond Function

Work	Year	Category	Secondary Category
[136]	2018	Communicate	P - Awareness and Training
[138]	2021	Improvements	R - Communicate
[137]	2019	Improvements	-

about cybersecurity threats and responses" [138] as well as the aspect that they investigate how these communication networks and their use can be *improved*. The study looked at communication across three levels: micro ((between individuals), meso (between organisations) and macro (across the whole domestic industry) and found that trust is one of the main factors in determining the organisation of the communication networks used and described by the participants.

Cooperative Cyber-Defence is an essential strategy in the fight against cyberattacks [137]. Sharing of information across various organisations can leverage the knowledge and information available to build a proactive defence system. Two challenges arise in connection with the information sharing. Firstly, an issue brought up in multiple works covered in this chapter, is the reluctance of organisations to share private information with outsiders. Secondly once a solution for the sharing of information is found the cyber threat information must be processed in such way to be able to train a model that can be used for future prediction of an unknown future cyber incident.

[137] propose a protocol that preserves the privacy of the organisation so that they can share their private information in an encrypted form. Specifically, a decision tree algorithm is proposed where organisations can build and subsequently learn based on training data aggregated from all other organisations. The algorithm is implemented to classify emails into spam or ham. The protocol proposed in [137] can be used only for datasets with features in the form of numerical values, as the homomorphic encryption used cannot be used to fractional numbers. This work can also be of relevance in the Detect step, however given the emphasis put on learning from past threats detected it seems fitting to categorize it to the Improvements subsection of Recover.

5.2.6 Conclusions

Finally, as discussed previously, the table outlining the search results gives a good indication of what is to follow, most of the research published so far focuses on the first three layers of the NIST Cybersecurity Framework: Identify, Protect and Detect. Much less research so far focuses on the Respond and Recover layers. However, the lines between stages are occasionally blurred, and a topic such as vulnerability disclosure can be included in a number of stages. Firstly, it can be part of the Detect layer, as it is concerned with finding out about vulnerabilities. It can also be part of the Respond layer as it could be considered voluntarily sharing information with external stakeholders, so the knowledge reaches a larger public. Finally, it could be part of the Recover function, because it relates to improvements that can be made in the future.

5.3 Solution Type taxonomy

Due to the breadth of the topic of cooperation and collaboration in cybersecurity extensive literature was produced. As discussed previously the literature varies with studies trying to identify factors which are related to the development of a cybersecurity culture across an organisation and the difficulties faced regarding the communication and collaboration on the topic [71] to much more technical approaches such as collision avoidance algorithms for autonomous ships, and in particular the exchange of information and interactions between ships [72].

Table 5.8: Literature classification based on the technical vs. non-technical criteria

Solution type	Number of Papers
Technical	33
Non-technical	21

Consequently, a different way to classify the literature is by whether the proposal is technical and non-technical. In the context of this report, technical means that the papers are proposing an implementation or a technical solution, such as algorithms [99], [100]. In contrast, non-technical solutions include organisational or human aspects, for instance frameworks or proposals for processes [73], [74], suggestions for loss mitigation [88] or frameworks on topics that are generally not implementing technical solutions, such as law [89].

Table 5.8 shows the split between the two categories, with technical solutions being more common than non-technical ones. It is worth noting that the topic does not necessarily have an impact on the classification of the paper, as such, information sharing or vulnerability sharing, for instance, was discussed both in technical works [108], [109] and in non-technical ones [81], [82].

Bringing the two previously discussed taxonomies together, NIST and solution type, we can see that there are certain patterns in the combined taxonomy. In Figure 5.10 it can be seen that the topics of Identify and Recover include relatively more non-technical papers, whereas the Protect, Detect and Respond functions include relatively more technical papers. An explanation for this is the character of the function itself. For example, the Identify function, includes categories such as governance and business environment, which are inherently non-technical topics, whereas the Detect function includes categories such as Anomalies and Events, where technical solutions need to be used to complete the task.

5.4 Function Type Taxonomy

Despite the popularity of the NIST framework, certain aspects create confusion. Terminology, for once is not clear and intuitive, Identify is not concerned with identification of

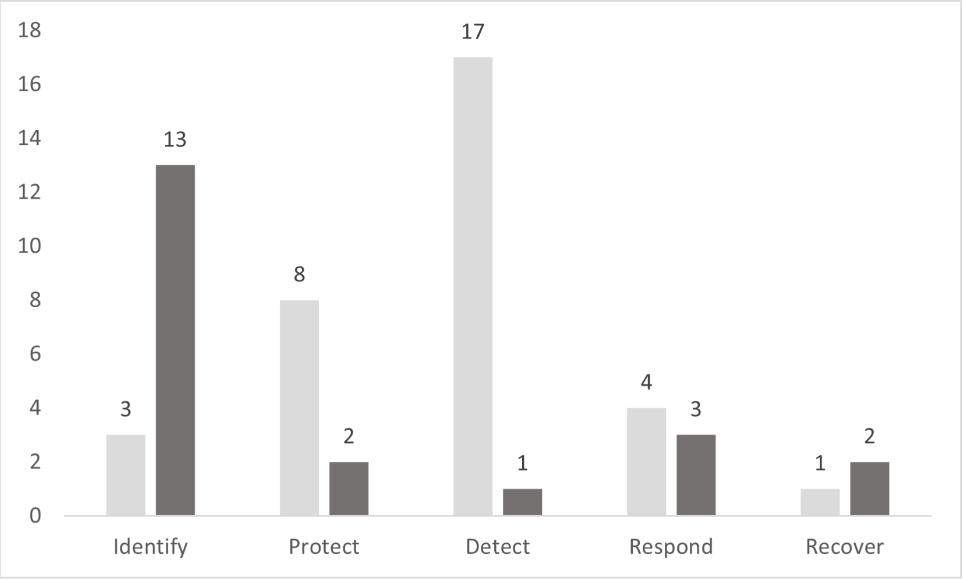


Figure 5.10: Literature classification based on solution type

attacks, but with identification of assets, processes and other aspects that need to be protected. Furthermore, Communication and Improvements are categories belonging both to the Respond and Recover functions. Therefore, based on the NIST framework, but with slight changes, a third taxonomy is proposed dividing the literature into 3 categories: *(i)* Governance, here the focus is on frameworks, processes and policies. *(ii)* Identifying attacks and *(iii)* Protective Measures. Table 5.5 gives an overview of what category each paper belongs to.

Figure 5.11 gives an overview of how this taxonomy compares to the NIST one. The colour of the circles represent NIST categories: orange are papers belonging to the Identify function, blue for Protect function, pink for Detect function, green for Respond function and finally, purple for the Recover function. Overall, it can be seen that the categorisation broadly follows the NIST one, with some exceptions. Additionally, connections represented by dotted lines have been drawn between papers which cover related topics, such as threat modelling and risk assessment. Finally, three additional concepts based on which papers were clustered together are introduced: Access Control, Intrusion Detection System and Information Sharing. This is to show directions where relatively more literature exists. To highlight how the same topic can be covered by multiple NIST functions, Information Sharing can be observed. It connects to papers from all three functions: governance, attack identification and protective measures. Additionally based on colour, we can see that it connects to literature part of the Identify, Recover, Respond and Detect NIST funtions. These overlaps serve as an example of the interconnectivity of cybersecurity topics based on collaboration and cooperation.

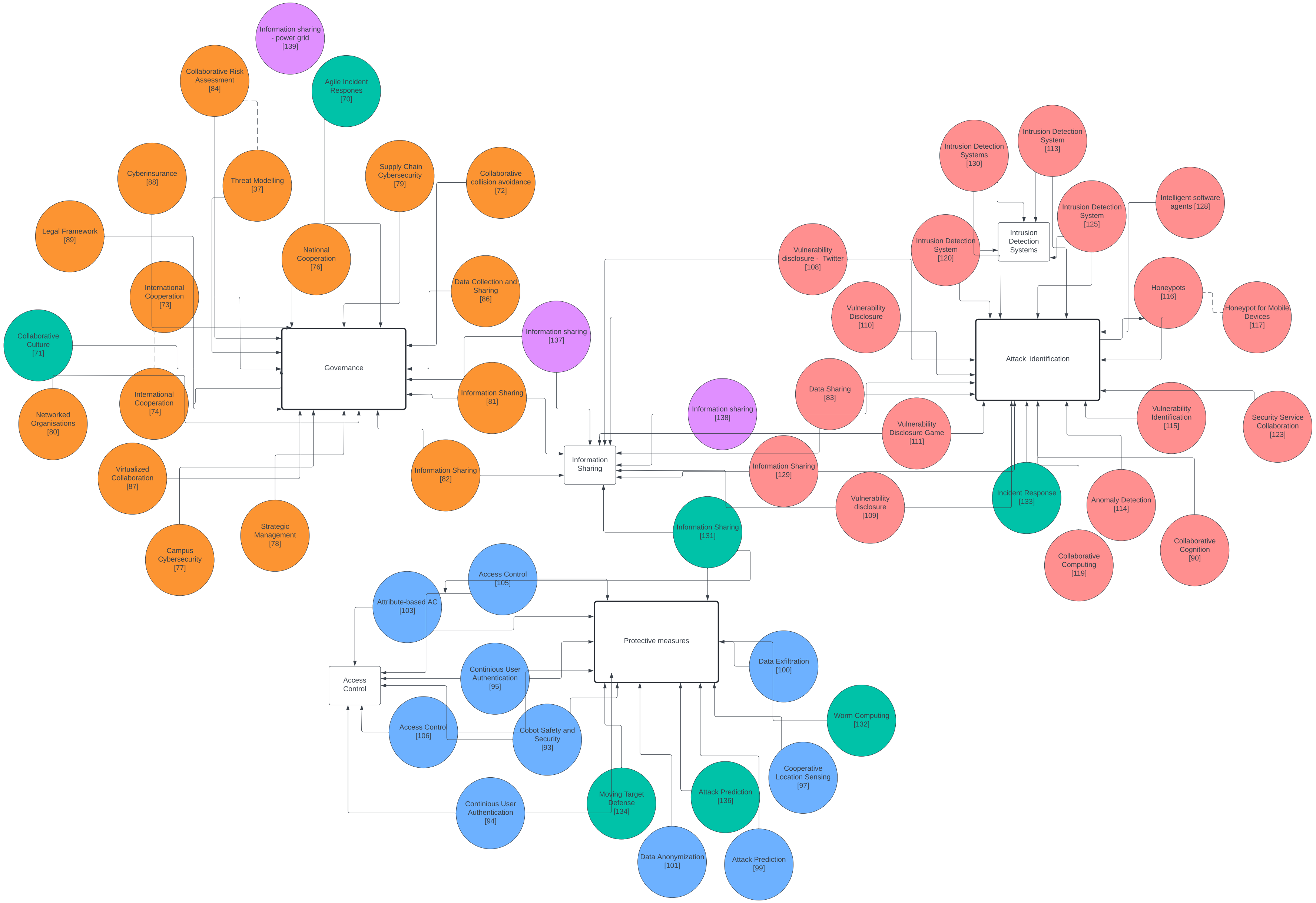

Information sharing - power grid [139]
Collaborative Risk Assessment [84]
Agile Incident Respones [70]
Cyberinsurance [88]
Threat Modelling [37]
Supply Chain Cybersecurity [79]
Collaborative collision avoidance [72]
Legal Framework [89]
National Cooperation [76]
International Cooperation [73]
Data Collection and Sharing [86]
Collaborative Culture [71]
Governance
Information sharing [137]
International Cooperation [74]
Information Sharing [81]
Networked Organisations [80]
Virtualized Collaboration [87]
Information Sharing [82]
Campus Cybersecurity [77]
Strategic Management [78]
Information Sharing
Intrusion Detection Systems [130]
Intrusion Detection System [113]
Intrusion Detection Systems
Intrusion Detection System [125]
Intelligent software agents [128]
Vulnerability disclosure - Twitter [108]
Intrusion Detection System [120]
Honeypots [116]
Honeypot for Mobile Devices [117]
Vulnerability Disclosure [110]
Attack identification
Data Sharing [83]
Information sharing [138]
Vulnerability Disclosure Game [111]
Vulnerability Identification [115]
Security Service Collaboration [123]
Information Sharing [129]
Vulnerability disclosure [109]
Incident Response [133]
Anomaly Detection [114]
Information Sharing [131]
Collaborative Computing [119]
Collaborative Cognition [90]
Access Control [105]
Attribute-based AC [103]
Protective measures
Data Exfiltration [100]
Access Control
Continious User Authentication [95]
Worm Computing [132]
Access Control [106]
Cobot Safety and Security [93]
Cooperative Location Sensing [97]
Moving Target Defense [134]
Attack Prediction [136]
Continious User Authentication [94]
Data Anonymization [101]
Attack Prediction [99]

Figure 5.11: Relationship NIST and function type classification

5.5 Collaboration Type Taxonomy

A final type of classification is based on the type of collaboration proposed. A division was made between collaboration among humans, across humans and machines and collaboration among machines. The latter includes solutions based on machine learning models, collaborative network architecture, or any solution that does not require direct human interaction. One point to note regarding the human machine collaboration is that this can be further split into human-computer and human-robot interactions. The literature discussed in this chapter addresses both, however they were pooled together for this classification as the emphasis is on the interaction between humans and machines and not on specificities regarding the machines. Table 5.9 shows the split between the three categories. Overall, the first two collaboration types are relatively more prevalent.

Table 5.9: Literature classification based on collaboration type

Human	Human-Machine	Machine
[73] 2017	[81] 2013	[72] 2022
[74] 2017	[84] 2019	[101] 2019
[77] 2022	[37] 2022	[99] 2021
[76] 2020	[87] 2021	[97] 2019
[106] 2018	[95] 2020	[108] 2020
[78] 2021	[94] 2021	[109] 2020
[79] 2020	[93] 2022	[113] 2019
[80] 2020	[100] 2020	[114] 2022
[111] 2022	[103] 2019	[116] 2021
[86] 2020	[105] 2021	[117] 2014
[83] 2015	[110] 2021	[119] 2018
[82] 2012	[115] 2022	[120] 2019
[88] 2015	[129] 2019	[123] 2017
[89] 2018	[131] 2016	[125] 2017
[70] 2022	[134] 2018	[128] 2007
[71] 2019	[137] 2019	[130] 2014
[136] 2018		[132] 2021
[138] 2021		[133] 2018
[90] 2018		[135] 2020

Chapter 6

Limitations, Challenges and Opportunities

6.1 Limitations

One of the limitations of this study is the number of surveyed papers relative to the available literature. However, the amount of material included in this work is sufficient to offer an overview of current directions in the literature. As with literature reviews and mapping studies, relevant papers might have been left out. Firstly *edge* literature, which does not explicitly mention collaboration, cooperation or cybersecurity could have been overlooked. Secondly due to the enormous amount of literature which does mention the relevant combination of terms, the decision to restrict the number of papers investigated (*cf.*, Chapter 4) might have led to exclusion of relevant papers.

The taxonomy and classification proposed inevitably have a subjective component. Furthermore, the classification of papers to fit the proposed taxonomy also have a subjective component. The subjective bias was minimised by providing explanations and clarifications for the decisions made where opportunity for disagreement was identified. Overall, the scope of this work was to propose a taxonomy and categorise existing literature according to it, however there certainly is not only one right way to do it. On the contrary given the extensive literature, there are a multitude of possible taxonomies to be discovered.

Finally, the surveyed literature often used collaboration and cooperation interchangeably making it difficult to apply the definitions proposed in this work. As such, no taxonomy was proposed distinguishing between these two distinct ways of working together, however literature including both concepts was used for the development of the proposed taxonomies and in the literature survey.

6.2 Challenges and Opportunities

Transparency in cybersecurity is paradoxical. As shown extensively in this work, collaboration can provide useful solutions and aide at solving issues much faster than without collaboration. However, an often-cited concern for organisations is sharing of information. And rightfully so. While transparency can help mend off attacks by enabling collaboration and cooperation to identify vulnerabilities, it can also tip off malicious parties to the existence of issues before these are resolved. Furthermore, sharing information after an attack, while useful for learning how to avoid a similar attack in the future, could also reveal too much information about the systems of the organisation. Indeed a few of the surveyed papers do address this issue and hopefully in the future more can be done to provide reassurance to organisations that sharing information is more helpful than harmful.

Collaborations between the private and public sector, including government and law enforcement can certainly be beneficial, but also have their limitations. There can be a certain level of mistrust between the two differing sectors. For instance, the lack of trust between the government and large technology companies. The issue of transparency mentioned earlier is even more acute in the case of private and public sector, with the amount of information that governments are willing to share being limited because of concerns over government security. Moreover, data privacy is a further concern that has lately been raised more by the public as well. Finally, the differences in culture, mandate and language between the public and private sector can hinder the cooperation. While organisations are concerned with profitability, the government is more focused on the legislative aspects of cybersecurity [140].

A considerable number of papers surveyed used machine learning (ML) techniques to tackle cybersecurity issues, and opportunities in the field are still numerous. According to [141] 42.3% of security professionals have a strong preference to use ML in cybersecurity, and 43% percent have a moderate preference. These findings highlight further that ML and data science are regarded as useful and helpful for cybersecurity. Identifying areas where ML can be implemented in a collaborative way constitutes a great opportunity for the future.

Finally humans and machines can very well team up in cybersecurity operations to improve results. To achieve this, it is necessary for machines to understand how to provide decision support the human counterparties, hence they must be built on behavioural and cognitive models [142]. However ultimately many of the requirements for a successful human-machine collaboration are like any other analytic work. The understanding of the user's goals and an awareness of its activities, an ability to provide flexible responded to needs that are abstractly formulated and the learning and adaptation capacity to changing circumstances [142]. How to achieve this in cybersecurity operations is potential future work topic.

In terms of further work on taxonomies there are a number of topics where further opportunities become apparent. Intrusion detection systems, vulnerability and information sharing, access control and human-computer interactions in particular have a large amount of dedicated literature. Based on the findings of this work, there is enough literature connected to collaboration and cooperation on the four topics mentioned previously to warrant dedicated taxonomies.

To conclude this chapter areas of the NIST framework [6] where little literature has been identified will be discussed from the perspective of an organisation. This case study shall serve as guidance for future work on collaboration and cooperation in cybersecurity.

Identify There are still aspects of identifying what needs to be protected that have not been investigated. In the category of *Asset management* methods for collaborative or cooperative work should still be identified. This step would involve identifying data, devices, personnel, and systems that would need to be protected and managed accordingly to their importance for the organisation. Taking just a few examples, organisational data flows and communications patterns could be mapped collaboratively across teams to understand where vulnerabilities might arise. Cybersecurity responsibilities for the entire workforce should be established. This is in itself a collaborative endeavour requiring coordination across the organisation, and collaborative frameworks or procedures could be implemented.

From the perspective of the *Business Environment* the organisation should understand its objectives, stakeholders, and activities. Based on this understanding, its cybersecurity roles, responsibilities, and risk management decisions should be based. For example, collaborative processes can be established to understand the organisation's place in the critical infrastructure, its dependencies, and relevant functions for delivering critical services. Finally collaborative methods to establish the role of the organisation within its supply chain could be investigated.

Additionally, the entire *Supply Chain Risk Management* should be understood. This is another area that is inherently cooperative, as organisations must interact with other entities in the supply chain - would they not interact, they would not be part of a supply chain. Here again, policies and frameworks could be established to identify, assess, and find ways to manage the cyber supply chain risks. This would also require a good understanding of all the supply chain collaborators and providers of components, services, and information systems. Finally, assessments of partners need to be made routinely, to confirm that they are meeting contractual obligations with regards to cybersecurity. Contracts themselves can be based on collaborative legal cybersecurity frameworks, similar to that proposed in [89].

Protect With regards to this function, organisations should ensure that their employees and partners are given good *Cybersecurity Awareness Education* and are taught to fulfil their duties related to cybersecurity in line with the policies, procedures, and agreements. This includes users with privileges, third-party stakeholders and senior managers understanding their roles and responsibilities. Here, there could be collaboration across different organisations to provide the best education between partnering organisation and create a network of collaborators which are aware of cyber risks and vulnerabilities. Another option would be synergies between the organisation and the public sector in the area of education.

Data Security can also be approached collaboratively. Data must be protected at rest and in transit. Data at rest can be protected through collaborative access control or encryption, while in transit data can be protected by asymmetric key encryption. Finally, *Information Protection Processes and Procedures* shall be enforced. These can use cooperative or collaborative methods to ensure that a baseline configuration for the information technology is proposed and maintained based on security principles. Moreover, backup of information and data should be conducted, maintained, and tested. This can be done cooperatively, as proposed in [143], [144].

Respond The organisation shall implement a *Response plan* to be executed in case of an incident. This should include processes and procedures and can be based on collaboration, to ensure security incidents are responded to promptly. An important aspect of responding to an attack is represented by *Communication*. This serves as a basis for coordination or response activities across internal and external stakeholders, including those in the public sector and the law enforcement agencies. Communication includes creating a plan for personnel to know their roles and order of operations and to know who to contact and coordinate with in case of incidents.

Analysis is conducted to ensure the correct response and recovery activities are performed. The analysis includes multiple aspects. organisations should investigate notifications from detection systems. As presented in the literature survey there are a number of detection systems based on collaboration and cooperation. Forensics should be performed to understand the impact of the incident. Finally, incidents can be categorised accordingly to the response plan. Here collaborative methods for categorisations can be used.

Processes should be set up to receive, analyse and respond to disclosed vulnerabilities from external and internal sources, this implies collaboration with internal testing teams, security researchers and usage of information shared through security bulletins. The organisation shall itself report incidents and disclose them through a method of choice to collaborators. Finally, based on the detection and response activities, *Improvements* should be made to existing response plans and response strategies. Furthermore, improvements to collaboration in the context of response to incidents can be made.

Recover While communications from the perspective of the respond function are related to how to answer to an incident in the most efficient way, in the context of recovering from an incident, *Communication* refers to managing the public relations and reputation. This can be performed through collaboration with third parties or by the organisation on its own. Recovery activities must be communicated and coordinated across internal and external stakeholders as well as to management teams.

A further aspect of recovery is cyberinsurance. While one article was identified on the topic, there is potential for much more research on the topic. Insurance does not only cover the financial or economic aspect of recovery but can also tackle reputational damage and other negative aspects in the aftermath of an incident.

Improvements can also be made from the recovery perspective, as the recovery planning and processes can be improved based on the lessons learned from incidents. Recovery strategies shall be updated. For instance, collaborative recovery processes with partners can be implemented in the aftermath of events [145].

The proposals above are based on the NIST Cybersecurity Framework [6]. No suggestions on the Detect function have been made, as this function is already very well covered in the literature. Additionally, since popular topics such as intrusion detection and vulnerability sharing all belong to the Detect function, research will likely be dedicated to the function in the future as well.

To conclude, there is multitude of areas in which collaboration and cooperation can be investigated in the context of cybersecurity. Given the varied types of collaborations, across humans in teams, between humans and computers or robots and across systems, effectively every function and category of the NIST framework can be addresses through collaboration or cooperation. However, despite the focus of this work on the aspects of cooperation and collaboration, and the fact that these certainly can bring improvements in some areas, solutions and proposals based on the two concepts are not necessarily always better. Therefore, the solutions, frameworks, processes etc. should always take into consideration whether collaboration and cooperation bring any improvements, and not mindlessly pursue collaboration for the sake of it.

Chapter 7

Summary and Conclusions

With cyberattacks posing a threat to the continuity and success of organisations worldwide [1] and the costs associated with cybersecurity skyrocketing in the last years. The need for appropriate cybersecurity has never been higher. And while malicious parties are teaming up to collaborate and cooperate on attacks, it is only natural that defenders should also cooperate or collaborate with each other to detect vulnerabilities or mitigate attacks.

The goals of this work were multiple. The current state of cybersecurity and important concepts and frameworks were discussed. In addition, based on literature related to cybersecurity as well as to collaboration and cooperation, definitions were formulated for collaborative cybersecurity and cooperative cybersecurity.

In a next step, four main research questions were answered. *Q1* relates to what interactions between cybersecurity, collaboration and cooperation have been investigated so far. Here the findings show that research is available in a multitude of areas, as different from each other as legal frameworks from ship navigation. *Q2* addressed patterns in the literature, here, the initial pattern identified was based on the five NIST functions. *Q3* related to a taxonomy to categorise existing literature was answered through the proposal of four classifications: based on the NIST framework, on the solution type (technical or non-technical), on the function type (governance, identifying attacks, or protection against them) and on the type of collaboration and cooperation used (among humans only, among computers only, or across humans and computers). Finally, to answer *Q4* a survey of the literature was conducted, and the fifty-four selected works were classified based on the proposed taxonomy.

Finally, limitations of the work as well as opportunities and challenges were identified. Additionally, a case study was introduced to present areas of the NIST framework where gaps in the literature were identified. These shall serve as a basis for future work.

Bibliography

[1] *The Cost of Cybercrime - Ninth Annual Cost of Cybercrime Study - Unloacking the Value of IMproved Cybersecurity Protection*, `https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf`, Last visit Jul 16, 2022.

[2] *Federal Bureau of Investigation- Internet Crime Report 2021*, `https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf`, Last visit Jul 16, 2022.

[3] *Investors put cybersecurity top of the business threat list*, `https://www.pwc.com/kz/en/pwc-news/what-new/investors-put-cybersecurity.html\#:~:text=Cyber\%20attacks\%20are\%20the\%20now,a\%20new\%20study\%20by\%20PwC.`, Last visit Jul 20, 2022.

[4] *DDoS Attacks Hit All-time High*, `https://www.infosecurity-magazine.com/news/ddos-attacks-hit-alltime-high/\#:~:text=The\%20number\%20of\%20distributed\%20denial,final\%20three\%20months\%20of\%202021.`, Last visit Jul 20, 2022.

[5] *Report: buying your own malware has never been easier*, `https://cybernews.com/security/buying-your-own-malware-has-never-been-easier/`, Last visit Jul 20, 2022.

[6] N. I. of Standards and Technology, "Cybersecurity framework version 1.0", U.S. Department of Commerce, Washington, D.C., Tech. Rep., 2014.

[7] M. Hentea, *Building an Effective Security Program for Distributed Energy Resources and Systems.* John Wiley & Sons, 2021.

[8] *The Fourth Industrial Revolution: what it means, how to respond*, `https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/`, Last visit Mar 13, 2022.

[9] ISO, "Iso/iec 27000:2018", *Information technology — Security techniques — Information security management systems — Overview and vocabulary*, 2018.

[10] M. Dlamini, J. Eloff, and M. Eloff, "Information security: The moving target", *Computers Security*, vol. 28, no. 3, pp. 189–198, 2009, ISSN: 0167-4048. DOI: `https://doi.org/10.1016/j.cose.2008.11.007`. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S0167404808001168`.

[11] ISO, "Iso/iec 27032:2012", *Information technology — Security techniques — Guidelines for cybersecurity*, 2012.

[12] D. Craigen, N. Diakun-Thibault, and R. Purse, “Defining cybersecurity”, *Technology Innovation Management Review*, vol. 4, no. 10, 2014.

[13] D. C. Wilson, *Cybersecurity*. MIT Press, 2021.

[14] M. Warkentin and C. Orgeron, “Using the security triad to assess blockchain technology in public sector applications”, *International Journal of Information Management*, vol. 52, p. 102 090, 2020, ISSN: 0268-4012. DOI: https://doi.org/10.1016/j.ijinfomgt.2020.102090. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S026840121930060X.

[15] D. Zissis and D. Lekkas, “Securing e-government and e-voting with an open cloud computing architecture”, *Government Information Quarterly*, vol. 28, no. 2, pp. 239–251, 2011, ISSN: 0740-624X. DOI: https://doi.org/10.1016/j.giq.2010.05.010. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0740624X10001383.

[16] A. Charle and F. Fulea, *AirGapped Key Management in a Remote Electronic Voting System*, 2022.

[17] N. I. of Standards and Technology, “Fips 200”, *Minimum Security Requirements for Federal Information and Information Systems*, 2006.

[18] L. O. Nweke, “Using the cia and aaa models to explain cybersecurity activities”, *PM World Journal*, vol. 6, no. 12, pp. 1–3, 2017.

[19] W. Smith, “A comprehensive cybersecurity defense framework for large organizations”, Ph.D. dissertation, Nova Southeastern University, 2019.

[20] S. Sowmya, P. Deepika, and J. Naren, “Layers of cloud–iaas, paas and saas: A survey”, *International Journal of Computer Science and Information Technologies*, vol. 5, no. 3, pp. 4477–4480, 2014.

[21] D. Freet, R. Agrawal, S. John, and J. J. Walker, “Cloud forensics challenges from a service model standpoint: Iaas, paas and saas”, in *Proceedings of the 7th International Conference on Management of computational and collective intElligence in Digital EcoSystems*, 2015, pp. 148–155.

[22] D. A. Wheeler and G. N. Larsen, “Techniques for cyber attack attribution”, INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA, Tech. Rep., 2003.

[23] V. Pham and T. Dang, “Cvexplorer: Multidimensional visualization for common vulnerabilities and exposures”, in *2018 IEEE International Conference on Big Data (Big Data)*, 2018, pp. 1296–1301. DOI: 10.1109/BigData.2018.8622092.

[24] *National Vulnerability Database Dashboard*, https://nvd.nist.gov/general/nvd-dashboard, Last visit Jul 18, 2022.

[25] *OWASP Top Ten*, https://owasp.org/www-project-top-ten/, Last visit Apr 03, 2022.

[26] *Real-World Examples for OWASP Top 10 Vulnerabilities*, https://www.cyberdb.co/real-world-examples-for-owasp-top-10-vulnerabilities, Last visit Jul 27, 2022.

[27] *OWASP Top 10 Vulnerabilities*, https://www.veracode.com/security/owasp-top-10, Last visit Jul 27, 2022.

[28] *Real Life Examples of Web Vulnerabilities (OWASP Top 10)*, `https://www.horangi.com/blog/real-life-examples-of-web-vulnerabilities`, Last visit Jul 27, 2022.

[29] *ENISA Threat Landscape 2021*, `https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021`, Last visit Jul 4, 2022.

[30] P. Pols and J. van den Berg, "The unified kill chain", *CSA Thesis, Hague*, pp. 1–104, 2017.

[31] M. Hajizadeh, N. Afraz, M. Ruffini, and T. Bauschert, "Collaborative cyber attack defense in sdn networks using blockchain technology", in *2020 6th IEEE Conference on Network Softwarization (NetSoft)*, 2020, pp. 487–492. DOI: `10.1109/NetSoft48620.2020.9165396`.

[32] K. Huang, M. Siegel, and S. Madnick, "Systematically understanding the cyber attack business: A survey", *ACM Computing Surveys (CSUR)*, vol. 51, no. 4, pp. 1–36, 2018.

[33] S. Murdoch and N. Leaver, "Anonymity vs. trust in cyber-security collaboration", in *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, 2015, pp. 27–29.

[34] E. A. Henneman, J. L. Lee, and J. I. Cohen, "Collaboration: A concept analysis", *Journal of advanced Nursing*, vol. 21, no. 1, pp. 103–109, 1995.

[35] S. Paul and C. Q. Peterson, "Interprofessional collaboration: Issues for practice and research", *Occupational Therapy In Health Care*, vol. 15, no. 3-4, pp. 1–12, 2002. DOI: `10.1080/J003v15n03\_01`.

[36] D. Freshwater, G. Sherwood, and V. Drury, "International research collaboration: Issues, benefits and challenges of the global network", *Journal of Research in Nursing*, vol. 11, no. 4, pp. 295–303, 2006.

[37] J. von der Assen, M. F. Franco, C. Killer, E. J. Scheid, and B. Stiller, "Coretm: An approach enabling cross-functional collaborative threat modeling", in *IEEE International Conference on Cyber Security and Resilience*, Virtually, Europe: IEEE, Jul. 2022, pp. 1–8.

[38] A. Al-Abri, Y. Jamoussi, N. Kraiem, and Z. Al-Khanjari, "Comprehensive classification of collaboration approaches in e-learning", *Telematics and Informatics*, vol. 34, no. 6, pp. 878–893, 2017.

[39] *What is Collaboration? A Complete Guide to Collaboration in 2022*, `https://kissflow.com/digital-workplace/collaboration/what-is-collaboration/`, Last visit Apr 15, 2022.

[40] K. R. Polenske, "Competition, collaboration and cooperation: An uneasy triangle in networks of firms and regions", in *Regional Competitiveness*, Routledge, 2012, pp. 45–60.

[41] N. Arnold, L. Ducate, and C. Kost, "Collaboration or cooperation? analyzing group dynamics and revision processes in wikis", *Calico Journal*, vol. 29, no. 3, pp. 431–448, 2012.

[42] T. M. Paulus, "Collaboration or cooperation? analyzing small group interactions in educational environments", in *Computer-supported collaborative learning in higher education*, IGI Global, 2005, pp. 100–124.

[43] G. Meng, Y. Liu, J. Zhang, A. Pokluda, and R. Boutaba, "Collaborative security: A survey and taxonomy", *ACM Computing Surveys (CSUR)*, vol. 48, no. 1, pp. 1–42, 2015.

[44] M. Usman, M. A. Jan, X. He, and J. Chen, "A survey on representation learning efforts in cybersecurity domain", *ACM Computing Surveys (CSUR)*, vol. 52, no. 6, pp. 1–28, 2019.

[45] M. Gimenez-Aguilar, J. M. de Fuentes, L. Gonzalez-Manzano, and D. Arroyo, "Achieving cybersecurity in blockchain-based systems: A survey", *Future Generation Computer Systems*, vol. 124, pp. 91–118, 2021, ISSN: 0167-739X. DOI: `https://doi.org/10.1016/j.future.2021.05.007`. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S0167739X21001576`.

[46] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, "Cybersecurity awareness in the context of the industrial internet of things: A systematic literature review", *Computers in Industry*, vol. 137, p. 103 614, 2022, ISSN: 0166-3615. DOI: `https://doi.org/10.1016/j.compind.2022.103614`. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S0166361522000094`.

[47] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities", *Sustainable Cities and Society*, vol. 50, p. 101 660, 2019, ISSN: 2210-6707. DOI: `https://doi.org/10.1016/j.scs.2019.101660`. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S2210670718316883`.

[48] Ž. Turk, B. G. de Soto, B. R. Mantha, A. Maciel, and A. Georgescu, "A systemic framework for addressing cybersecurity in construction", *Automation in Construction*, vol. 133, p. 103 988, 2022.

[49] M. Macas, C. Wu, and W. Fuertes, "A survey on deep learning for cybersecurity: Progress, challenges, and opportunities", *Computer Networks*, vol. 212, p. 109 032, 2022, ISSN: 1389-1286. DOI: `https://doi.org/10.1016/j.comnet.2022.109032`. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S1389128622001864`.

[50] S. Haque and G. Loukas, "Machine learning based prediction versus human-as-a-security-sensor", *International Journal of Artificial Intelligence Research*, vol. 3, Dec. 2018. DOI: `10.29099/ijair.v3i1.83`.

[51] R. Iniesta, D. Stahl, and P. Mcguffin, "Machine learning, statistical learning and the future of biological research in psychiatry", *Psychological Medicine*, vol. -1, pp. 1–11, Jul. 2016. DOI: `10.1017/S0033291716001367`.

[52] U. Michelucci, M. Baumgartner, and F. Venturini, "Optical oxygen sensing with artificial intelligence", *Sensors*, vol. 19, p. 777, Feb. 2019. DOI: `10.3390/s19040777`.

[53] *Machine Learning for SQL - Process Overview*, `https://docs.oracle.com/en/database/oracle/machine-learning/oml4sql/21/mlsql/process-overview.html\#GUID-628EF12F-57D4-476A-844B-0461C47918DF`, Last visit Jul 3, 2022.

[54] J. Pawlick, E. Colbert, and Q. Zhu, “A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy”, *ACM Comput. Surv.*, vol. 52, no. 4, 2019, ISSN: 0360-0300. DOI: 10.1145/3337772. [Online]. Available: https://doi.org/10.1145/3337772.

[55] R. E. Navas, F. Cuppens, N. Boulahia Cuppens, L. Toutain, and G. Z. Papadopoulos, “Mtd, where art thou? a systematic review of moving target defense techniques for iot”, *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 7818–7832, 2021. DOI: 10.1109/JIOT.2020.3040358.

[56] B. A. Kitchenham, D. Budgen, and P. Brereton, *Evidence-based software engineering and systematic reviews*. CRC press, 2015, vol. 4.

[57] T. Olsson, M. Hell, M. Höst, U. Franke, and M. Borg, “Sharing of vulnerability information among companies – a survey of swedish companies”, in *2019 45th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, 2019, pp. 284–291. DOI: 10.1109/SEAA.2019.00051.

[58] T. Tagarev and Y. Yanakiev, “Business models of collaborative networked organisations: Implications for cybersecurity collaboration”, in *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2020, pp. 431–438. DOI: 10.1109/DESSERT50317.2020.9125011.

[59] A. Sarma, A. van der Hoek, and L.-T. Cheng, “A need-based collaboration classification framework”, Jan. 2004.

[60] J. Webb and D. Hume, “Campus iot collaboration and governance using the nist cybersecurity framework”, in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018, pp. 1–7. DOI: 10.1049/cp.2018.0025.

[61] *Cybersecurity Framework Usage Graph (cropped)*, https://www.nist.gov/image/cybersecurityframeworkuseinfographiccroppedjpg, Last visit Jul 16, 2022.

[62] R. E. Navas, F. Cuppens, N. B. Cuppens, L. Toutain, and G. Z. Papadopoulos, “Mtd, where art thou? a systematic review of moving target defense techniques for iot”, *IEEE internet of things journal*, vol. 8, no. 10, pp. 7818–7832, 2020.

[63] H. S. Lallie, L. A. Shepherd, J. R. Nurse, *et al.*, “Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic”, *Computers Security*, vol. 105, p. 102 248, 2021, ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2021.102248. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821000729.

[64] *COVID-19 Risks Outlook A Preliminary Mapping and Its Implications*, https://www3.weforum.org/docs/WEF_COVID_19_Risks_Outlook_Special_Edition_Pages.pdf, Last visit Jul 16, 2022.

[65] *National Cybersecurity Center*, https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen.html, Last visit Jul 16, 2022.

[66] *Strategic Principles for Securing the Internet of Things (IoT)*, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf, Last visit Jul 16, 2022.

[67] *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*, `https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot`, Last visit Jul 16, 2022.

[68] *IoT Security Privacy Trust Framework v2.5*, `https://www.internetsociety.org/wp-content/uploads/2018/05/iot_trust_framework2.5a_EN.pdf`, Last visit Jul 16, 2022.

[69] M. Mylrea, S. N. G. Gourisetti, and A. Nicholls, "An introduction to buildings cybersecurity framework", in *2017 IEEE symposium series on computational intelligence (SSCI)*, IEEE, 2017, pp. 1–7.

[70] Y. He, E. D. Zamani, S. Lloyd, and C. Luo, "Agile incident response (air): Improving the incident response process in healthcare", *International Journal of Information Management*, vol. 62, p. 102 435, 2022.

[71] M. Ioannou, E. Stavrou, and M. Bada, "Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination", in *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, IEEE, 2019, pp. 1–4.

[72] M. Akdağ, P. Solnør, and T. A. Johansen, "Collaborative collision avoidance for maritime autonomous surface ships: A review", *Ocean Engineering*, vol. 250, p. 110 920, 2022.

[73] G. Lkhagvasuren, "Cybersecurity cooperation of countries: Impact of draft international code of conduct for information security", in *Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance*, 2017, pp. 564–565.

[74] Y. Cho and J. Chung, "Bring the state back in: Conflict and cooperation among states in cybersecurity", *Pacific Focus*, vol. 32, no. 2, pp. 290–314, 2017. DOI: `https://doi.org/10.1111/pafo.12096`.

[75] *U.S. Emergency Alert System*, `https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public/emergency-alert-system`, Last visit Jul 19, 2022.

[76] A. Woszczynski, A. Green, K. Dodson, and P. Easton, "Zombies, sirens, and lady gaga–oh my! developing a framework for coordinated vulnerability disclosure for us emergency alert systems", *Government Information Quarterly*, vol. 37, no. 1, p. 101 418, 2020.

[77] M. Bannister, "Collaboration and advance planning across campus create more cybersecure universities", *Campus Security Report*, vol. 18, no. 11, pp. 8–11, 2022. DOI: `https://doi.org/10.1002/casr.30915`. eprint: `https://onlinelibrary.wiley.com/doi/pdf/10.1002/casr.30915`. [Online]. Available: `https://onlinelibrary.wiley.com/doi/abs/10.1002/casr.30915`.

[78] R. Rajan, N. P. Rana, N. Parameswar, S. Dhir, Y. K. Dwivedi, *et al.*, "Developing a modified total interpretive structural model (m-tism) for organizational strategic cybersecurity management", *Technological Forecasting and Social Change*, vol. 170, p. 120 872, 2021.

[79] J. Simon and A. Omar, “Cybersecurity investments in the supply chain: Coordination and a strategic attacker”, *European Journal of Operational Research*, vol. 282, no. 1, pp. 161–171, 2020.

[80] T. Tagarev, “Governance of collaborative networked organisations: Stakeholder requirements”, in *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, IEEE, 2020, pp. 439–445.

[81] J. L. Hernandez-Ardieta, J. E. Tapiador, and G. Suarez-Tangil, “Information sharing models for cooperative cyber defence”, in *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, IEEE, 2013, pp. 1–28.

[82] W. Zhao and G. White, “A collaborative information sharing framework for community cyber security”, in *2012 IEEE Conference on Technologies for Homeland Security (HST)*, IEEE, 2012, pp. 457–462.

[83] J. Freudiger, E. De Cristofaro, and A. Brito, “Controlled data sharing for collaborative predictive blacklisting”, *arXiv preprint arXiv:1502.05337*, 2015.

[84] J. Lamp, C. E. Rubio-Medrano, Z. Zhao, and G.-J. Ahn, “Exsol: Collaboratively assessing cybersecurity risks for protecting energy delivery systems”, in *2019 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, IEEE, 2019, pp. 1–6.

[85] *Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid*, `https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/`, Last visit Jul 20, 2022.

[86] A. Atapour-Abarghouei, A. S. McGough, and D. S. Wall, “Resolving the cybersecurity data sharing paradox to scale up cybersecurity via a co-production approach towards data sharing”, in *2020 IEEE International Conference on Big Data (Big Data)*, IEEE, 2020, pp. 3867–3876.

[87] F. Kilger, A. Kabil, V. Tippmann, G. Klinker, and M.-O. Pahl, “Detecting and preventing faked mixed reality”, in *2021 IEEE 4th International Conference on Multimedia Information Processing and Retrieval (MIPR)*, IEEE, 2021, pp. 399–405.

[88] P. H. Meland, I. A. Tondel, and B. Solhaug, “Mitigating risk with cyberinsurance”, *IEEE Security & Privacy*, vol. 13, no. 6, pp. 38–43, 2015.

[89] J. Kosseff, “Developing collaborative and cohesive cybersecurity legal principles”, in *2018 10th International Conference on Cyber Conflict (CyCon)*, IEEE, 2018, pp. 283–298.

[90] S. N. Narayanan, A. Ganesan, K. Joshi, T. Oates, A. Joshi, and T. Finin, “Early detection of cybersecurity threats using collaborative cognition”, in *2018 IEEE 4th international conference on collaboration and internet computing (CIC)*, IEEE, 2018, pp. 354–363.

[91] J. Noll, O. Bojang, and S. Rietjens, “Deterrence by punishment or denial? the efp case”, in *NL ARMS Netherlands Annual Review of Military Studies 2020*, TMC Asser Press, The Hague, 2021, pp. 109–128.

[92] H. Zhu, *E-CARGO and Role-based Collaboration: Modeling and Solving Problems in the Complex World*. John Wiley & Sons, 2021.

[93] M. Gleirscher, N. Johnson, P. Karachristou, R. Calinescu, J. Law, and J. Clark, "Challenges in the safety-security co-assurance of collaborative industrial robots", in *The 21st Century Industrial Robot: When Tools Become Collaborators*, Springer, 2022, pp. 191–214.

[94] S. S. Almohamade, J. A. Clark, and J. Law, "Behaviour-based biometrics for continuous user authentication to industrial collaborative robots", in *Innovative Security Solutions for Information Technology and Communications: 13th International Conference, SecITC 2020, Bucharest, Romania, November 19–20, 2020, Revised Selected Papers*, 2020, pp. 185–197.

[95] S. Almohamade, J. Clark, and J. Law, "Continuous user authentication for human-robot collaboration", in *The 16th International Conference on Availability, Reliability and Security*, ser. ARES 2021, Vienna, Austria: Association for Computing Machinery, 2021, ISBN: 9781450390514. DOI: 10.1145/3465481.3470025. [Online]. Available: https://doi.org/10.1145/3465481.3470025.

[96] F. Maggi, D. Quarta, M. Pogliani, M. Polino, A. M. Zanchettin, and S. Zanero, "Rogue robots: Testing the limits of an industrial robot's security", *Trend Micro, Politecnico di Milano, Tech. Rep*, pp. 1–21, 2017.

[97] Z. Wang, S. Wang, M. Z. A. Bhuiyan, J. Xu, and Y. Hu, "Cooperative location-sensing network based on vehicular communication security against attacks", *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–11, 2022. DOI: 10.1109/TITS.2022.3160453.

[98] R. Ko and R. Choo, *The cloud security ecosystem: technical, legal, business and management issues.* Syngress, 2015.

[99] L. Tang, F. Li, and J. Li, "Research on internet of vehicles attack prediction based on federated learning", in *2021 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS)*, IEEE, 2021, pp. 574–578.

[100] M.-H. Chung, M. Chignell, L. Wang, A. Jovicic, and A. Raman, "Interactive machine learning for data exfiltration detection: Active learning with human expertise", in *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, IEEE, 2020, pp. 280–287.

[101] K.-S. Wong, N. A. Tu, D.-M. Bui, S. Y. Ooi, and M. H. Kim, "Privacy-preserving collaborative data anonymization with sensitive quasi-identifiers", in *2019 12th CMI Conference on Cybersecurity and Privacy (CMI)*, IEEE, 2019, pp. 1–6.

[102] R. S. Sandhu and P. Samarati, "Access control: Principle and practice", *IEEE communications magazine*, vol. 32, no. 9, pp. 40–48, 1994.

[103] Y. Xue, K. Xue, N. Gai, J. Hong, D. S. Wei, and P. Hong, "An attribute-based controlled collaborative access control scheme for public cloud storage", *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 11, pp. 2927–2942, 2019.

[104] S. Yu, M. Li, and L. Shi, "Chapter 6.3 - trust establishment in wireless body area networks", in *Wearable Sensors*, E. Sazonov and M. R. Neuman, Eds., Oxford: Academic Press, 2014, pp. 475–491, ISBN: 978-0-12-418662-0. DOI: https://doi.org/10.1016/B978-0-12-418662-0.00011-8. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780124186620000118.

[105] J. Park, R. Sandhu, M. Gupta, and S. Bhatt, "Activity control design principles: Next generation access control for smart and collaborative systems", *IEEE Access*, vol. 9, pp. 151 004–151 022, 2021.

[106] Y.-H. Chen and P.-C. Huang, "Collaborative access control of cloud storage systems", in *2018 IEEE International Conference on Applied System Invention (ICASI)*, IEEE, 2018, pp. 1063–1064.

[107] A. Pala and J. Zhuang, "Information sharing in cybersecurity: A review", *Decision Analysis*, vol. 16, no. 3, pp. 172–196, 2019.

[108] H. Shin, W. Shim, J. Moon, J. W. Seo, S. Lee, and Y. H. Hwang, "Cybersecurity event detection with new and re-emerging words", in *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, ser. ASIA CCS '20, Taipei, Taiwan: Association for Computing Machinery, 2020, pp. 665–678, ISBN: 9781450367509. DOI: `10.1145/3320269.3384721`. [Online]. Available: `https://doi.org/10.1145/3320269.3384721`.

[109] A. N. M. B. Rashid, M. Ahmed, L. F. Sikos, and P. Haskell-Dowland, "Anomaly detection in cybersecurity datasets via cooperative co-evolution-based feature selection", *ACM Trans. Manage. Inf. Syst.*, vol. 13, no. 3, Feb. 2022, ISSN: 2158-656X. DOI: `10.1145/3495165`. [Online]. Available: `https://doi.org/10.1145/3495165`.

[110] A. Bahl, A. Sharma, and M. R. Asghar, "Vulnerability disclosure and cybersecurity awareness campaigns on twitter during covid-19", *SECURITY AND PRIVACY*, vol. 4, no. 6, e180, 2021. DOI: `https://doi.org/10.1002/spy2.180`.

[111] D. Cohen, A. Elalouf, and R. Zeev, "Collaboration or separation maximizing the partnership between a "gray hat" hacker and an organization in a two-stage cybersecurity game", *International Journal of Information Management Data Insights*, vol. 2, no. 1, p. 100 073, 2022, ISSN: 2667-0968. DOI: `https://doi.org/10.1016/j.jjimei.2022.100073`. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S2667096822000167`.

[112] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review", *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.

[113] A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review", *WIREs Data Mining and Knowledge Discovery*, vol. 9, no. 4, e1306, 2019.

[114] X. Han, Y. Zhou, K. Chen, *et al.*, "Ads-lead: Lifelong anomaly detection in autonomous driving systems", *IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS*, 2022.

[115] M. M. Thwe, Z. M. Belay, E. Jee, and D.-H. Bae, "Cybersecurity vulnerability identification in system-of-systems using model-based testing", in *2022 17th Annual System of Systems Engineering Conference (SOSE)*, IEEE, 2022, pp. 317–322.

[116] D. Zhuravchak, T. Ustyianovych, V. Dudykevych, B. Venny, and K. Ruda, "Ransomware prevention system design based on file symbolic linking honeypots", in *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, IEEE, vol. 1, 2021, pp. 284–287.

[117] E. Vasilomanolakis, S. Karuppayah, M. Mühlhäuser, and M. Fischer, "Hostage: A mobile honeypot for collaborative defense", in *Proceedings of the 7th International Conference on Security of Information and Networks*, ser. SIN '14, Glasgow, Scotland, UK: Association for Computing Machinery, 2014, pp. 330–333, ISBN: 9781450330336. DOI: 10.1145/2659651.2659663. [Online]. Available: https://doi.org/10.1145/2659651.2659663.

[118] *Unified Cyber Ontology*, https://unifiedcyberontology.org/, Last visit Jul 20, 2022.

[119] E. Oyekanlu, "Osmotic collaborative computing for machine learning and cybersecurity applications in industrial iot networks and cyber physical systems with gaussian mixture models", in *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, IEEE, 2018, pp. 326–335.

[120] T. G. Nguyen, T. V. Phan, B. T. Nguyen, C. So-In, Z. A. Baig, and S. Sanguanpong, "Search: A collaborative and intelligent nids architecture for sdn-based cloud iot networks", *IEEE access*, vol. 7, pp. 107 678–107 694, 2019.

[121] *Software-Defined Networking*, https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html, Last visit Jul 20, 2022.

[122] *What is SDN?*, https://www.ciena.com/insights/what-is/What-Is-SDN.html, Last visit Jul 20, 2022.

[123] D. Migault, M. A. Simplicio, B. M. Barros, *et al.*, "A framework for enabling security services collaboration across multiple domains", in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, IEEE, 2017, pp. 999–1010.

[124] *What Is Network Service Chaining? Definition?*, https://www.sdxcentral.com/networking/sdn/definitions/whats-network-virtualization/what-is-network-service-chaining/, Last visit Jul 20, 2022.

[125] S. Teng, N. Wu, H. Zhu, L. Teng, and W. Zhang, "Svm-dt-based adaptive and collaborative intrusion detection", *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 1, pp. 108–118, 2017.

[126] *Support Vector Machine — Introduction to Machine Learning Algorithms*, https://towardsdatascience.com/support-vector-machine-introduction-to-machine-learning-algorithms-934a444fca47, Last visit Aug 01, 2022.

[127] *Decision Trees in Machine Learning*, https://towardsdatascience.com/decision-trees-in-machine-learning-641b9c4e8052, Last visit Aug 01, 2022.

[128] D. Edwards, S. Simmons, and N. Wilde, "Prevention, detection and recovery from cyber-attacks using a multilevel agent architecture", in *2007 IEEE International Conference on System of Systems Engineering*, IEEE, 2007, pp. 1–6.

[129] M. Liu, Z. Xue, X. He, and J. Chen, "Cyberthreat-intelligence information sharing: Enhancing collaborative security", *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 17–22, 2019.

[130] Z. Tan, U. T. Nagar, X. He, *et al.*, "Enhancing big data security with collaborative intrusion detection", *IEEE cloud computing*, vol. 1, no. 3, pp. 27–33, 2014.

[131] R. Garrido-Pelaz, L. González-Manzano, and S. Pastrana, “Shall we collaborate? a model to analyse the benefits of information sharing”, ser. WISCS ’16, Vienna, Austria: Association for Computing Machinery, 2016, pp. 15–24, ISBN: 9781450345651. DOI: `10.1145/2994539.2994543`. [Online]. Available: `https://doi.org/10.1145/2994539.2994543`.

[132] L. Shi, X. Li, Z. Gao, P. Duan, N. Liu, and H. Chen, “Worm computing: A blockchain-based resource sharing and cybersecurity framework”, *Journal of Network and Computer Applications*, vol. 185, p. 103 081, 2021.

[133] J. Steinberger, B. Kuhnert, C. Dietz, *et al.*, “Ddos defense using mtd and sdn”, in *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*, IEEE, 2018, pp. 1–9.

[134] C. Zhong, J. Yen, P. Liu, and R. F. Erbacher, “Learning from experts’ experience: Toward automated cyber security data triage”, *IEEE Systems Journal*, vol. 13, no. 1, pp. 603–614, 2018.

[135] M. Husák and P. Čeleda, “Predictions of network attacks in collaborative environment”, in *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium*, IEEE, 2020, pp. 1–6.

[136] M. He, L. Devine, and J. Zhuang, “Perspectives on cybersecurity information sharing among multiple stakeholders using a decision-theoretic approach”, *Risk Analysis*, vol. 38, no. 2, pp. 215–225, 2018.

[137] S. Badsha, I. Vakilinia, and S. Sengupta, “Privacy preserving cyber threat information sharing and learning for cyber defense”, in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, 2019, pp. 0708–0714.

[138] R. G. Randall and S. Allen, “Cybersecurity professionals information sharing sources and networks in the us electrical power industry”, *International Journal of Critical Infrastructure Protection*, vol. 34, p. 100 454, 2021.

[139] *Moving Target Defense*, `https://www.dhs.gov/science-and-technology/csd-mtd`, Last visit Aug 01, 2022.

[140] *Can public private partnerships tackle growing cybersecurity concerns?*, `https://earlymetrics.com/can-public-private-partnerships-tackle-growing-cybersecurity-concerns/`, Last visit Aug 22, 2022.

[141] S.-L. Peng, G. Suseendran, and D. Balaganesh, *Intelligent Computing and Innovation on Data Science.* Springer, 2020.

[142] C. Lyn Paul, L. M. Blaha, C. K. Fallon, C. Gonzalez, and R. S. Gutzwiller, “Opportunities and challenges for human-machine teaming in cybersecurity operations”, in *Proceedings of the human factors and ergonomics society annual meeting*, SAGE Publications Sage CA: Los Angeles, CA, vol. 63, 2019, pp. 442–446.

[143] M.-O. Killijian, L. Courtès, and D. Powell, “A survey of cooperative backup mechanisms”, 2006.

[144] S. Elnikety, M. Lillibridge, M. Burrows, and W. Zwaenepoel, “Cooperative backup system”, in *The USENIX Conference on File and Storage Technologies*, 2002.

[145] K.-F. Cheung, M. G. Bell, and J. Bhattacharjya, “Cybersecurity in logistics and supply chain management: An overview and future research directions”, *Transportation Research Part E: Logistics and Transportation Review*, vol. 146, p. 102 217, 2021.

List of Figures

List of Tables