



## Horizon 2020 Program (2014-2020)

Cybersecurity, Trustworthy ICT Research & Innovation Actions

Security-by-design for end-to-end security

H2020-SU-ICT-03-2018



Cyber security cOmpeteNcE fOr Research anD InnovAtion<sup>†</sup>

### Work package 4: Policy and the European dimension

#### Deliverable D4.3: 3<sup>rd</sup> Year Report on Cybersecurity Threats

**Abstract:** Building on the 1st year report (Deliverable D4.1) on cybersecurity threats, the present Deliverable provides an advanced overview of the cybersecurity threat landscape from a technological, legal/policy, and economic perspective. The discussion surfaces existing gaps and challenging points at practices associated with implementing cybersecurity at an organizational level. It also provides a refined recommendation on cybersecurity threats (*e.g.*, countermeasures, challenges, and state-of-the-art solutions), which started to be defined in the 2nd year report (Deliverable D4.2). Thus, this 3rd-year report (Deliverable D4.3) constitutes the outcome of specific activities, which took place in 2021, including work (a) on countermeasures and research actions from a technical perspective, (b) the development of cybersecurity cultures and updates on the existing and upcoming regulatory landscape, and (c) the definition of relevant steps for a guideline and approach to reach an economically efficient investment decision in cybersecurity.

Contractual date of delivery	<i>31.12.2021</i>
Actual date of delivery	<i>22.12.2021</i>
Deliverable dissemination level	<i>Public</i>
Editors	<i>Muriel Franco, Burkhard Stiller (UZH)</i>
Contributors	<i>Muriel Franco, Eder Scheid, Burkhard Stiller (UZH), Claudio Ardagna, Marco Anisetti, Nicola Bena, Ernesto Damiani (UMIL), Arthur van der Wees, Dimitra Stefanatou, Giacomo Delinavelli (ALBV), Aljosa Pasic, Jose Ruiz (ATOS)</i>
Quality assurance	<i>eesy-inno, NCSA, UP, and CUT</i>

<sup>††</sup> This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927.

**The CONCORDIA Consortium**

UniBW/CODE	University Bundeswehr Munich / Research Institute CODE (Coordinator)	Germany
FORTH	Foundation for Research and Technology - Hellas	Greece
UT	University of Twente	Netherlands
SnT	University of Luxembourg	Luxembourg
UL	University of Lorraine	France
UM	University of Maribor	Slovenia
UZH	University of Zurich	Switzerland
JACOBSUNI	Jacobs University Bremen	Germany
UI	University of Insubria	Italy
CUT	Cyprus University of Technology	Cyprus
UP	University of Patras	Greece
TUBS	Technical University of Braunschweig	Germany
TUDA	Technical University of Darmstadt	Germany
MU	Masaryk University	Czech Republic
BGU	Ben-Gurion University	Israel
OsloMET	Oslo Metropolitan University	Norway
Imperial	Imperial College London	UK
UMIL	University of Milan	Italy
BADW-LRZ	Leibniz Supercomputing Centre	Germany
EIT DIGITAL	EIT DIGITAL	Belgium
TELENOR ASA	Telenor ASA	Norway
AirbusCS-GE	Airbus Cybersecurity GmbH	Germany
SECUNET	secunet Security Networks AG	Germany
IFAG	Infineon Technologies AG	Germany
SIDN	Stichting Internet Domeinregistratie Nederland	Netherlands
SURF	SURF BV	Netherlands
CYBER-DETECT	Cyber-Detect	France
TID	Telefonica I+D SA	Spain
RUAG	RUAG AG (as a replacement for RUAG Schweiz AG)	Switzerland
BITDEFENDER	Bitdefender SRL	Romania
ATOS	Atos Spain S.A.	Spain
SAG	Siemens AG	Germany
Flowmon	Flowmon Networks AS	Czech Republic
TÜV TRUST IT	TUV TRUST IT GmbH	Germany
TI	Telecom Italia SPA	Italy
Efacec	EFACEC Electric Mobility SA (as a replacement for EFACEC Energia)	Portugal
ARTHUR'S LEGAL	Arthur's Legal B.V.	Netherlands
eesy-inno	eesy-innovation GmbH	Germany
DFN-CERT	DFN-CERT Services GmbH	Germany
CAIXABANK SA	CaixaBank SA	Spain
BMW Group	Bayerische Motoren Werke AG	Germany
NCSA	Ministry of Digital Governance - National Cyber Security Authority	Greece
RISE	RISE Research Institutes of Sweden AB	Sweden

Ericsson	Ericsson AB	Sweden
SBA	SBA Research gemeinnützige GmbH	Austria
IJS	Institut Jozef Stefan	Slovenia
UiO	University of Oslo	Norway
ULANC	University of Lancaster	UK
ISI	ATHINA-ISI	Greece
UNI PASSAU	University of Passau	Germany
RUB	Ruhr University Bochum	Germany
CRF	Centro Ricerche Fiat	Italy
ELTE	EOTVOSLORANDTUDOMANYEGYETEM	Hungary
Utimaco	Utimaco Management GmbH	Germany
FER	University of Zagreb, Faculty of Electrical Engineering and Computing	Croatia

## Document Revisions & Quality Assurance

### Internal Reviewers

1. Anja Majstorovic (eesy-inno) (review lead)
2. George Drivas (NCSA)
3. Konstantinos Lampropoulos (UP)
4. Michael Sirivianos (CUT)

### Revisions

<b>Ver.</b>	<b>Date</b>	<b>By</b>	<b>Overview</b>
0.01	18.02.2021	UZH	Initial structure and Methodology
0.02	31.03.2021	UZH, UMIL, ALBV	Inclusion of planned sections per task leader
0.03	01.08.2021	UZH	Economic perspectives (initial organization)
0.04	01.09.2021	UMIL	Technical perspective (initial organization)
0.05	25.10.2021	UZH	Chapter 5 – Economic Perspectives
0.06	03.11.2021	UZH	Chapter 1 and Chapter 2, all content
0.07	10.11.2021	UMIL	Chapter 3 – Technical Perspectives and Appendices
0.08	10.11.2021	ALBV	Chapter 4 – Legal Perspectives, EU Strategies, and Code of Engagement (Appendices)
0.09	10.11.2021	ATOS	Chapter 5.2 - Cybersecurity Ecosystem Benefits
1.00	12.11.2021	UZH	Integration of all inputs, Executive Summary, Chapter 6, and editorial checks and completions
1.01	24.11.2021	UZH	Updates on Chapter 1 and Chapter 5 after reviews
1.02	26.11.2021	UMIL	Updates on Chapter 2 and Appendices after reviews
1.03	26.11.2021	ATOS	Updates on Chapter 5.2 after reviews
1.04	26.11.2021	ALBV	Updates on Chapter 1, Chapter 3, and Appendices after reviews
1.05	29.11.2021	UZH	Integration of all inputs and editorial checks for second round of internal review
1.06	07.11.2021	UZH	Updates on Economics Perspective after internal review
1.07	08.11.2021	ALBV	Updates on Legal Perspective after internal review
1.08	09.12.2021	ATOS	Updates on Chapter 5.2 after internal review
1.09	11.12.2021	UMIL	Updates on Technical Perspective after internal review
2.00	15.12.2021	UZH	Editorial work; Ready for submission

<i>2.01</i>	<i>27.05.2022</i>	<i>UZH</i>	<i>Editorial work after official review</i>
<i>2.02</i>	<i>06.06.2022</i>	<i>UMIL</i>	<i>Updates and extensions on Technical Perspectives</i>
<i>2.03</i>	<i>07.06.2022</i>	<i>UMIL, UZH</i>	<i>Mapping of WP1 and T4.1</i>
<i>3.00</i>	<i>10.06.2022</i>	<i>UZH</i>	<i>Final integration; ready for publication</i>

**Disclaimer:**

The sole responsibility of this document lies with the authors. The European Commission is not responsible for any use that may be made of the information contained therein.

## Executive Summary

Cyberattacks have changed and did evolve dramatically during recent years. In 2020, the COVID-19 pandemic also accelerated these changes, with people and services being even further digitized and with wider-range Home Office setting. This digital dependence of society, governments, and companies now emphasizes the importance of the CONCORDIA project and, especially, this deliverable, since it sheds light on cyber threats, their impacts, and countermeasures from a technical, legal, and economic perspective. CONCORDIA focused on the analysis of cyber threats from key dimensions: technical, legal, and economic perspectives. These perspectives provide a deep insight into major challenges and novel solutions proposed to address open issues within selected domains of cybersecurity, especially the device/IoT-, network-, system-, data-, application-, and user-centric domains. All analyses and results summarized and detailed herein are provided by experts in each of these perspectives covered.

At first, the key challenges for the EU and respective strategies to build cybersecurity sovereignty are defined. To determine the possible interplay in a fixed setting, the CONCORDIA environment and its stakeholders are defined as well. In turn, the newest details on cybersecurity threats in their technical perspectives are described by mapping current and future EU cybersecurity research actions, focusing on those six domains, as stated above. Besides, an extensive analysis of cybersecurity threats, challenges and countermeasures are dissected and recommended against these threats, including research actions and the most relevant aspects to dedicate efforts to protect systems and networks.

Secondly, the legal perspective provides an overview of the EU regulatory landscape from the point of view of cybersecurity. This overview captures both the most relevant regulations that are already applicable in EU, as well as the proposed regulations pertinent to CONCORDIA's scope, such as the Artificial Intelligence (AI) Act and the Data Governance Act (DGA). Moreover, the discussion elaborates on several principles relating to the implementation of digital sovereignty following from the series of follow-up interviews conducted in Year 2 with external stakeholders. Finally, the legal perspective provides for the rationale, the approach and the aims of the "Code of Engagement for Threat Intelligence Sharing", as captured under the latest version of the Code, initially, addressed to CONCORDIA community.

Thirdly, selected guidelines for cybersecurity planning and economic investments in cybersecurity threat countermeasures, focusing on main requirements especially, are outlined. In addition, a new model for a closely reviewed cyber insurance market is defined; it embraces cybersecurity economics, such as risk assessment using Machine Learning (ML), and decentralized solutions. Driven by measurable benefits of building a cybersecurity ecosystem, from a technical as well as economic point of view, strategies to stimulate essential collaborations are discussed. Thus, an analysis of economic aspects, especially covering incentives related to threat intelligence sharing, is provided.

Finally, a coherent set of remarks from these three viewpoints, influencing work on cybersecurity threats in general, cover a brief discussion about what potentially to expect in the next few years regarding EU-related cybersecurity efforts and research fields. Thus, a major argument is provided by which the sustainability of CONCORDIA's work within the Work Package WP4 on "Policy and the European Dimension" is foreseen. All WP4 activities in its three tasks proceeded as planned, includes collaborations within other CONCORDIA work packages. This work reported so far will continue to be applied to real-world scenarios within the last project year to come.

## Contents

<b>1. Introduction .....</b>	<b>9</b>
<b>1.1. The EU Cybersecurity Strategy.....</b>	<b>10</b>
1.1.1. Resilience, Technological Sovereignty, and Leadership.....	10
1.1.2. Building Operational Capacity to Prevent, Deter, and Respond .....	11
1.1.3. Advancing a Global and Open Cyberspace .....	12
<b>1.2. Methodology .....</b>	<b>13</b>
1.2.1. Technical Perspective.....	13
1.2.2. Legal Perspective.....	14
1.2.3. Economics Perspective .....	15
<b>1.3. Structure of this Document.....</b>	<b>16</b>
<b>2. The CONCORDIA Environment.....</b>	<b>17</b>
<b>2.1. Domains of Interest.....</b>	<b>17</b>
<b>2.2. Mapping of Stakeholders .....</b>	<b>18</b>
<b>3. Technical Perspectives: Cybersecurity Research Actions and Countermeasures.....</b>	<b>19</b>
<b>3.1. New Threats, Gaps, and Challenges .....</b>	<b>19</b>
3.1.1. Device/IoT-Centric Security.....	19
3.1.2. Network-Centric Security .....	20
3.1.3. System-Centric Security .....	22
3.1.4. Data-Centric Security.....	23
3.1.5. Application-Centric Security .....	24
3.1.6. User-Centric Security.....	24
<b>3.2. Countermeasures and Research Actions.....</b>	<b>25</b>
3.2.1. Device/IoT-Centric Security.....	25
3.2.2. Network-Centric Security .....	32
3.2.3. System-Centric Security .....	41
3.2.4. Data-Centric Security.....	47
3.2.5. Application-Centric Security .....	53
3.2.6. User-Centric Security.....	58
3.2.7. Cross-Cutting Countermeasures and Research Actions.....	63
<b>4. Legal Perspectives .....</b>	<b>66</b>
<b>4.1. Update on the Existing Regulatory Landscape.....</b>	<b>66</b>
4.1.1. The Directive on Security of Network and Information Systems (NIS Directive).....	67
4.1.2. The Regulation on ENISA and on Information and Communications Technology Cybersecurity Certification (Cybersecurity Act).....	68
4.1.3. General Data Protection Regulation (GDPR).....	69
4.1.4. The Regulation on the Free Flow of Non-Personal Data.....	70
4.1.5. Product Liability Directive (Liability for AI-enabled Products and Services).....	70
4.1.6. Radio Equipment Directive.....	71
4.1.7. Regulation for European Cybersecurity Competence Centre .....	72
<b>4.2. Update on the Upcoming Regulatory Landscape.....</b>	<b>73</b>
4.2.1. Artificial Intelligence Act (AI Act) .....	73
4.2.2. The Data Governance Act (DGA) .....	74
4.2.3. Digital Operational Resilience Act .....	76
4.2.4. Digital Services Act (DSA) and Digital Markets Act (DMA) .....	76
4.2.5. Resilience of Critical Entities Act (CER) .....	77
4.2.6. Other Legislative Initiatives.....	78
<b>4.3. Implementing Cybersecurity Principles: The Interview Series 2020.....</b>	<b>79</b>
4.3.1. From Why to How .....	79
4.3.2. Two Main Common Denominators in the Interview Series 2021 .....	80
4.3.3. Implementing Digital Sovereignty Principles: International Privacy Law Perspective .....	81
4.3.4. Implementing Digital Sovereignty Principles: Accountability perspective .....	82
4.3.5. Implementing Digital Sovereignty Principles: Policy Making Perspective .....	83
4.3.6. Implementing Digital Sovereignty Principles: AI Tooling Perspective .....	84
4.3.7. Implementing Digital Sovereignty Principles: University Lecturer Perspective.....	84
<b>4.4. The Code of Engagement for Threat Intelligence Sharing.....</b>	<b>85</b>

<b>5. Economic Perspectives .....</b>	<b>86</b>
<b>5.1. Cyber Insurance (CI) Market and Models .....</b>	<b>90</b>
5.1.1. Overview of Cyber Insurance Steps and the Framework Definition.....	91
5.1.2. Stakeholders and Relationships.....	92
5.1.3. SaCI: a Blockchain-based Cyber Insurance Model.....	95
<b>5.2. Cybersecurity Ecosystem Benefits .....</b>	<b>99</b>
5.2.1. Cybersecurity Ecosystem Specificities.....	100
5.2.2. Related Work.....	100
5.2.3. Gaps and Challenges.....	102
5.2.4. Stakeholder Analysis .....	102
5.2.5. Strategies to Stimulate Production of EU Cybersecurity Technology in an Ecosystem .....	103
5.2.6. Economic Issues in Threat Intelligence Sharing .....	104
<b>5.3. Kirti: Decentralized Reputation and SLA Enforcement for Cybersecurity .....</b>	<b>111</b>
5.3.1. Kirti's Overview .....	112
5.3.2. Case Study: Usage of Kirti in the Cybersecurity Market.....	114
5.3.3. Discussions on Costs, Decentralization, and Rating Fraud .....	116
<b>5.4. SecRiskAI: ML-based Tool for Cybersecurity Risk Assessment.....</b>	<b>118</b>
5.4.1. Conceptual Architecture of SecRiskAI .....	118
5.4.2. Risk Assessment Workflow, Data Gathering, and Processing .....	120
5.4.3. Multi-Class ML Classification Algorithms.....	124
5.4.4. MENTOR'S API Integration .....	128
5.4.5. Discussion and Limitations .....	129
<b>6. Summary and Final Remarks .....</b>	<b>130</b>
<b>6.1. Technical Views .....</b>	<b>130</b>
<b>6.2. Legal Views.....</b>	<b>131</b>
<b>6.3. Economic Views .....</b>	<b>132</b>
<b>References .....</b>	<b>133</b>
<b>Appendices .....</b>	<b>142</b>
<b>A. Threats, Gaps, Challenges, Countermeasures, Research Actions: Summary .....</b>	<b>142</b>
A.1. Device/IoT-Centric Security .....	142
A.2. Network-Centric Security.....	148
A.3. System-Centric Security.....	154
A.4. Data-Centric Security .....	160
A.5. Application-Centric Security.....	168
A.6. User-Centric Security .....	172
<b>B. Mapping Between Published Papers in WP1 and Gaps and Challenges .....</b>	<b>178</b>
B.1. Device-Centric Security .....	178
B.2. Network-Centric Security.....	179
B.3. Software-Centric Security .....	180
B.4. Application-Centric Security.....	181
B.5. Data and User-Centric Security.....	181
<b>C. Dynamic Code of Engagement for Trusted Threat Intelligence Sharing.....</b>	<b>184</b>

## 1. Introduction

As businesses become more digitized, they are exposed to an increasing number of threats, such as Distributed Denial-of-Service (DDoS) attacks, ransomware, and data breaches [1]. Thus, beyond compromising companies' and their customers' security and privacy, malicious attackers can negatively affect the economy of businesses or services supported by digital systems [2]. Predictions from the Cybersecurity Ventures, the world's leading researchers for the global cyber economy, indicate that cybercrime damages will hit € 8 trillion annually by 2025 [3]. Such damages include direct and indirect costs, *e.g.*, those involved with the loss of critical data, asset theft, business disruption, and reputation harm [4]. Hence, it is essential to think and plan about cybersecurity not only on the technical side, but also to consider especially economic and legal impacts of digital threats [5].

However, even with the rising number of cyberattacks, there often exists a wrong and misleading perception of risks and a lack of cybersecurity investments and awareness from different stakeholders. In many cases companies without security expertise in-house. Currently, Small and Medium-sized Enterprises (SME) are among the most affected companies in various sectors. For instance, according to the results of a recent survey [6], 63% of Chief Information Security Officers (CISO) managing small cyber security teams think that risks are higher in small companies (less than 250 employees) than in larger ones. Furthermore, as pointed in [7], SMEs often fail to evaluate their risks and underestimate impacts of cyberattacks on their businesses.

A recent joint work conducted by Concordia partners [8] was focused on the understanding and mapping the threat landscape of the – very dynamic – digital world. It was observed that threats are changing together with the evolution of the Information Technology (IT) environment; from pure software-based systems to the Internet-of-Things (IoT), via services and cloud computing. According to the European Union Agency for Cybersecurity (ENISA), a set of threats have emerged and were consolidated as the most critical ones during the last few years [9]. These threats include not only those focusing on system and application domains, like general Malware, Ransomware, and Cryptojacking, but also those targeting the human's good faith (*i.e.*, user-centric attacks), such as phishing and misinformation.

Thus, in order to address current and future threats for companies and society, it is important, in advance of an attack, to determine an efficient cybersecurity plan, which European stakeholders can adopt in order to avoid and mitigate threats that might have not have only technical, but also measurable economic and societal impacts. Within such a context, it is important to understand: (a) countermeasures from a technical view, (b) legal and regulatory directions, and (c) economic impacts of attacks to reach an efficient cybersecurity ecosystem in Europe. In this direction, the past Deliverables D4.1 as well as D4.2 and now D4.3 focus on important aspects of cybersecurity, its threats, and impacts, highlighting examples of countermeasures, which are possible today, and determining research areas for the next years.

## 1.1. The EU Cybersecurity Strategy

On 16 December 2020, the Commission published its new Cybersecurity Strategy for the Digital Decade (henceforth, in short “Strategy”)<sup>1</sup>. The Strategy discusses the pivotal role cybersecurity plays in the Commission’s agenda for building a resilient, green and digital Europe, namely for the achievement of the so-called “twin transitions”.<sup>2</sup>

The Strategy considers cybersecurity as an integral part of Europeans’ security. In this sense, the perspective is twofold: it concerns internal matters and external relations. Cybersecurity of internal matters is concerned with securing the continuous functioning of essential services, such as health care, energy, financial services, or transportation. With respect to external relations, cybersecurity concerns protection from threats and attacks coming from foreign actors, as well as upholding multilateralism on a global stage.

Cybersecurity also plays an important role in ensuring the smooth functioning of the European Digital Single Market. In this sense, the Strategy points out that concerns with respect to security are a major disincentive to using online services.<sup>3</sup> The Strategy is structured in three areas of action: (1) resilience, technological sovereignty and leadership; (2) building operational capacity to prevent, deter and respond; and (3) advancing global and open cyberspace. Each of these three areas of action is presented in the following.

### 1.1.1. Resilience, Technological Sovereignty, and Leadership

The Strategy addresses this area with a holistic approach, which includes the use of legal and policy initiatives, as well as investments directed at strengthening the quality and capabilities of the European cybersecurity community.

The legislative commitment in this area concerns the revision of the NIS directive, a new directive concerning the resilience of Critical Entities and the Digital Operational Resilience Act. The scope of these legislative initiatives concerns infrastructures, services and entities whose role is considered essential in the European economy. By setting specific standards of protection, the EU Commission aims at ensuring their “resilience” against cyberthreats. These proposals, together with the currently applicable legislation in the field of cybersecurity, will be discussed in further detail in Chapter 4 of this deliverable. The policy commitments in this area are concerned with a set of tools and initiatives, such as the 5G Toolbox, the EU cybersecurity certification framework, the Revised Digital Education Action Plan.

---

<sup>1</sup> European Commission, ‘Joint Communication to the European Parliament and the Council: The EU’s Cybersecurity Strategy for the Digital Decade’ (Brussels, 16 December 2020) 18 final. <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>

<sup>2</sup> European Commission, ‘Eco-innovation Action Plan’ (Brussels, 5 March 2021). [https://ec.europa.eu/environment/ecoap/about-eco-innovation/policies-matters/green-and-digital-twin-transition-also-spurs-inclusive-eco\\_en](https://ec.europa.eu/environment/ecoap/about-eco-innovation/policies-matters/green-and-digital-twin-transition-also-spurs-inclusive-eco_en)

<sup>3</sup> Directorate-General for Communication, ‘Special Eurobarometer 499: Europeans’ attitudes towards cyber security (cybercrime)’ [https://data.europa.eu/data/datasets/s2249\\_92\\_2\\_499\\_eng?locale=en](https://data.europa.eu/data/datasets/s2249_92_2_499_eng?locale=en)

The 5G Toolbox lays out a range of security measures aiming to effectively mitigate risks and ensure that secure 5G networks are deployed across Europe. It sets out detailed mitigation plans for each of the identified risks and recommends a set of key strategic and technical measures, which should be taken by all Member States and/or by the Commission.<sup>4</sup>

The EU cybersecurity certification framework provides for EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards, and procedures. The framework is based on an agreement at the level of the EU on the evaluation of the security properties of a specific ICT-based product or service. The aim is to attest that ICT products and services that have been certified in accordance with such a scheme comply with specified requirements.<sup>5</sup>

The Strategy also includes the Revised Digital Education Action Plan. The latter raises cybersecurity awareness among individuals, especially children and young people, and organizations, especially SMEs. It also aims to encourage women's participation in science, technology, engineering, and mathematics ('STEM'), education and ICT jobs upskilling and reskilling in digital skills.<sup>6</sup>

The EU is committed to support the Strategy through an unprecedented level of (public and private) investments over the next seven years (2021-2027). Investments from the EU should trigger (equal amounts of) investments from the Member States and the private industry, under a partnership co-governed with the Member States. These investments should be channeled through the Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN).<sup>7</sup>

The Commission proposes to build a network of Security Operations Centres (SOCs) across the EU, and to support the improvement of existing centres and the establishment of new ones. It will also support the training and skill development of staff operating these centres. The Commission intends to develop a contingency plan, supported by EU funding, for dealing with extreme scenarios affecting the integrity and availability of the global DNS root system. In this sense, the Strategy points at the development of a public European DNS resolver service (DNS4EU). This initiative will offer a European alternative service for accessing the global Internet.

### **1.1.2. Building Operational Capacity to Prevent, Deter, and Respond**

The Strategy addresses this area of intervention by pointing at existing or in the making tools of cooperation, enforcement, deterrence, and defence.

With regard to cooperation, the Strategy describes the Join Cyber Unit as a virtual and physical "platform" to enable the Member States and EU institutions, bodies and agencies

---

<sup>4</sup> European Commission, 'EU Toolbox for 5G Security' (Brussels, March 2021). [The EU toolbox for 5G security | Shaping Europe's digital future \(europa.eu\)](https://ec.europa.eu/digital-strategy/en/policies/cybersecurity-certification-framework)

<sup>5</sup> European Commission, 'The EU cybersecurity certification framework' (<https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework>)

<sup>6</sup> European Commission, 'Digital Education Action Plan (2021-2027) Resetting education and training for the digital age.' ([https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan\\_en](https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en))

<sup>7</sup> At the time of writing this deliverable, the institution under analysis has taken the name of European Cybersecurity Competence Centre and Network (ECCC). The Regulation establishing the ECCC will be analysed in section 4.2.7.

to make full use of existing structures, resources and capabilities and promote cybersecurity cooperation and a “need- to-share” mind-set.<sup>8</sup> In this sense, the Unit would act as a backstop where the participants can draw on one another’s support and expertise, especially in the event that various cyber communities are required to work closely together.

The Strategy also considers tackling cybercrime as a key factor in ensuring cybersecurity. In this sense, the Strategy points out at the strong level of cooperation between ENISA and Europol, and specifically to the pivotal role that the latter further play to support national law enforcement authorities combating cyber-enabled and cyber-dependent crime.<sup>9</sup>

The so-called cyber diplomacy toolbox defines another that the Strategy considers for averting and reacting to malicious cyber activities.<sup>10</sup> This instrument allows for the imposition of restrictive measures on individuals and entities involved or responsible for cyberattacks against the EU or the Member States, as well as to deliver a swift and effective joint EU diplomatic response to cyberthreats. This effort is coordinated by the High Representative of the Union for Foreign Affairs and Security Policy. The latter will also be aided by the establishment of a Member States’ EU cyber intelligence working group residing within the EU Intelligence and Situation Centre (INTCEN).

### 1.1.3. Advancing a Global and Open Cyberspace

The Strategy also considers the role that the EU can play on the international stage to advance open and secure cyberspace. The Strategy highlights the value of international and European standardization bodies as well as of standard development organizations. According to the Strategy, with and within these organizations, the EU should define its objectives for international standardization, and conduct proactive and coordinated outreach to promote these at the international level.

Moreover, the role of the EU on the international stage should not be limited to influencing the above-mentioned bodies, but engage with international fora, such as the UN, as well as with third countries and bodies such as the African Union, the ASEAN Regional Forum, the Organization of American States, and the Organization for Security Cooperation in Europe. In particular, the Strategy points at the EU-NATO cooperation, which should focus on cyberdefense interoperability requirements.

Besides strengthening diplomatic relations and exerting influence over international fora, the EU should continue to support its partners to increase their cyber resilience and capacities. According to the Strategy, the EU should develop an EU External Cyber Capacity Building Agenda to steer these efforts in line with its External Cyber Capacity Building Guidelines and the Agenda 2030 for Sustainable Development. In this sense, an EU Cyber Capacity Building Board shall be created to encompass relevant EU institutional stakeholders, and to monitor progress, as well as the identification of further synergies and potential gaps.

---

<sup>8</sup> European Commission, Joint Cyber Unit (<https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit>).

<sup>9</sup> European Commission, ‘Joint Communication to the European Parliament and the Council: The EU’s Cybersecurity Strategy for the Digital Decade’ (Brussels, 16 December 2020), page 15.

<sup>10</sup> CCDCOE, ‘European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox’ (<https://ccdcoe.org/incyber-articles/european-union-equipping-itself-against-cyber-attacks-with-the-help-of-cyber-diplomacy-toolbox/>)

## 1.2. Methodology

The Deliverable D4.3 is the last one of three consecutive Deliverables (*i.e.*, D4.1, D4.2, and D4.3) due at M12, M24, and M36, respectively. These three Deliverables focus on the analysis of cyberthreats from the technical (Task T4.1), legal (Task T4.2), and economic (Task T4.3) perspectives, thus, providing insights, discussing challenges, and describing novel solutions to address open issues within different domains of cybersecurity. All activities and analyses that are built around this Deliverable are provided by experts in each one of the perspectives covered by the Tasks T4.1, T4.2, and T4.3 below.

While the Deliverable D4.1 presented the first overview of cybersecurity threats, mainly focusing on the state-of-the-art in those domains of relevance (*e.g.*, User-, Application-, System-, Network-, and Device-centric) for CONCORDIA, the Deliverable D4.2 provided a view on the evolving cybersecurity landscape as well as the rise of threats during the COVID-19 pandemic. Thus and finally, Deliverable D4.3 focuses now on the analysis of countermeasures against threats mapped within D4.1 and D4.2 and provides research actions for those different domains of interest (*i.e.*, User, Application, System/Software, Network, Device-centric Security) for CONCORDIA.

### 1.2.1. Technical Perspective

Task T4.1 produced threat reports focusing on CONCORDIA's domains of interest (*cf.* Section 2.1) and established liaisons, while closely collaborating with relevant European experts and stakeholders to contribute to the cybersecurity roadmap for Europe within Task T4.4 as well.

Activities in T4.1 were composed out of three main phases. The first phase (emerging threats and evolving attacks) was conducted in the first year of the project and provided an overview of the current state-of-the-art on threats and cybersecurity in the CONCORDIA domains (*cf.* Section 2.1). This phase reported within Deliverable D4.1 collected relevant documents from literature, including white papers and reports (*e.g.*, ENISA threat landscape and Europol documents) and produced a snapshot of the status of cybersecurity, harmonizing knowledge from different activities and organizations. It evaluated the new trends in cybersecurity, focusing on emerging threats and evolving attacks.

The first phase provided an overview of assets, threats, and attacks, shaping current trends in cybersecurity. Next, the second phase (gaps and challenges) was reported within the Deliverable D4.2. It analyzed and discussed gaps and challenges concerning threats and vulnerabilities identified, and its managed crosscutting aspects of the threat landscape affecting further domains of interest. The third phase is reported within this deliverable at hand and provides finally a set of guidelines and an overview of existing countermeasures. Last, but not least, the list of research actions considered relevant as of today's perspective is also provided to shape future research to mitigate identified threats and their risks.

Summarizing, activities in T4.1 have been documented in three different Deliverables that provide the current overview of technological findings as follows:

- D4.1 presented a first threat analysis and state-of-the-art overview.

- D4.2 refined this threat analysis and focused on crosscutting aspects as well as gaps and challenges.
- D4.3 (this deliverable at hand) provides the final threat analysis and discussion on future research actions and countermeasures.

Activities within Task T4.1 built on the competencies of partners in CONCORDIA, benefiting from their direct contributions. To this aim, different working groups collaborated in the domains of (i) Device/IoT-centric, (ii) network-centric, (iii) system-centric, (iv) data-centric, (v) application-centric, and (vi) user-centric security. These working groups produced the relevant content for Chapter 3, elaborating on gaps and challenges in the area that each working group addressed.

### 1.2.2. Legal Perspective

In the spirit of a human-centric approach to cybersecurity, the legal perspective puts particular emphasis on organizational measures employed by organizations of all sizes participating in the project in view of ensuring compliance with those requirements set under EU law. Considering the regulatory landscape illustrated in Deliverable D4.1 and the reality of cybersecurity at an implementation level, the legal perspective produced a set of recommendations to strengthen the effectiveness of existing rules and to create an organizational culture around cybersecurity.

Notably, based on the planning concerning the legal perspective as elaborated within Deliverable D4.1, the Task T4.2 focused on the "state of play" concerning the most relevant regulations pertinent to cybersecurity and organizational practices (as performed within CONCORDIA's project years 1 and 2) in order to produce recommendations on how to reach the "state of the art" at the project's stage now (at the end of project year 3). Independent of that perspective, Task T4.2 delivered a set of early recommendations already within project year 2.

The work of Task T4.2 comprises both desk research and qualitative research in the form of interviews with consortium partners to be elaborated further in the discussion to follow below. In particular, while these interviews were conducted within project year 2 initially, representatives of sector-specific CONCORDIA pilots and from CONCORDIA's threat intelligence, specifically from certification perspectives, had been involved. In the context of these interviews, the COVID-19 pandemic has been addressed as well. Also, the development of a "Code of Engagement for Threat Intelligence Sharing" had been the focus on work Task T4.2 performed in the last project year.

Considering also the interdependencies of all tasks in WP4 as well as more specifically the resulting outcomes mentioned under the technological perspective depicted above, the legal perspective did capture the following:

1. D4.1 illustrated the regulatory environment by providing an overview of the most relevant already applicable and proposed regulations.
2. D4.2 produced an update of the regulatory developments and further addressed actual practices to safeguard cybersecurity at an organizational level. Based on input

collected directly from CONCORDIA partners, primarily from the sector-specific pilots, namely, from the aerospace sector, the e-health sector, the threat intelligence sector, and the financial sector, 11 D4.2 provided for a set of early recommendations.

3. D4.3 (this deliverable at hand) provides for a further update of the policy and regulatory developments that took place in Year 3. It, also, provides insights on how to implement digital sovereignty, by, essentially, strengthening cybersecurity in practice. To this end, the discussion below focuses on several principles of outstanding importance following from a series of interviews performed in Year 3 with external stakeholders. Furthermore, D4.3 provides for the latest version of the “Code of Engagement for Threat Intelligence Sharing” initially addressed to CONCORDIA community.

### 1.2.3. Economics Perspective

The economics perspective maps actors, responsibilities, inter-dependencies, and risks involved, relevant for cybersecurity to provide a measurable basis for economic analysis models, ready to analyse and determine measurable factors in the area of cybersecurity mechanisms. These models do provide an accurate picture of cybersecurity economic impacts, thus, helping stakeholders to analyse economic impacts of threats and the decision-making process toward an adequate level of cybersecurity. In addition, different stakeholders are identified by considering real-world scenarios, which include stakeholders that are more impacted by cyberattacks (*e.g.*, governments, companies, and the financial sector).

Thus, in the light of such information, a novel framework was proposed and reported in the Deliverable D4.1 for estimating costs in complex distributed systems. This framework provides detailed models for cost estimations and mapping relations between interdependent systems and their components. The D4.2 then, from an economic perspective, focused on providing new approaches (*e.g.*, visual tools, conversational agents, and recommender system) to support cybersecurity planning and investment.

Activities conducted within Task T4.3 provide outcomes for the set of WP4 Deliverables and dedicated activities within the CONCORDIA as follows:

- D4.1 provided a discussion about the economic impacts of cybersecurity and introduced initial steps for a risk assessment and analysis of cybersecurity investments. Moreover, based on highly specific threats and risks analyzed, a case study was performed on a dedicated ransomware scenario.
- D4.2 focused on the refinement of planning and investments steps for cybersecurity countermeasures, by providing new use cases under investigation. Also, a visualization tool was developed to support cybersecurity economics quantification and the related risk analysis.
- D4.3 (this deliverable at hand) provides final recommendations on economic perspectives, determines relevant steps for those cybersecurity planning and

---

<sup>11</sup> Notably, interviewees were informed that for the purpose of the performance of the specific interviews the Chatham House Rule would apply.

economic investments, especially with respect to SME demands, and discusses state-of-the-art approaches proposed to support such a decision-process of investments in cybersecurity so that to minimize the loss of businesses affected by cyberattacks. These approaches include the microeconomics of the cyber insurance market and measurable benefits of building a cybersecurity ecosystem, which include a discussion of strategies to stimulate essential collaborations such as those related to the threat intelligence sharing.

Overall, within project year 3, activities in Tasks T4.1, T4.2, and T4.3 did proceed as planned. The COVID-19 pandemic has been taken into account under the respective activities for project year 2, therefore, the Deliverable D4.2 encapsulates the impact of COVID-19 on the evolving cybersecurity threat landscape, which are now revisited with a certain degree in the Deliverable D4.3 at hand. Thus, Deliverable D4.3 focuses on major concerns, aspects of importance now, and emerging questions that have to be considered for today and the next years of cybersecurity, taking also into consideration changes in the digital world of recent years due to different reasons (*e.g.*, extension of remote and home office/work, the evolution of mobile communications, and rising ransomware and phishing attacks).

### **1.3. Structure of this Document**

Deliverable D4.3 is structured as follows.

Chapter 2 presents the important CONCORDIA environment focusing on domains of interest and stakeholders.

Chapter 3 presents the technological perspective of cybersecurity, focusing on new threats, gaps, and technical challenges. Also, countermeasures and research actions are highlighted.

Chapter 4 presents from a legal perspective the main recommendation on how to develop an organizational culture on cybersecurity while monitoring and updating the regulatory landscape.

Chapter 5 details the most important steps for cybersecurity planning and investment, including economic aspects of threat information sharing and novel tools developed to address a selected subset of those challenges related to economic aspects and impacts of cybersecurity, especially focusing on SMEs.

This deliverable concludes in Chapter 6 with a summary and final findings of these different, but interdependent perspectives (*i.e.*, technical, legal, and economic), including a proposed view into the next 1-3 years of cybersecurity research, operations, and challenges.

## 2. The CONCORDIA Environment

The CONCORDIA environment is a key to understand how the domains of interest are targeted within this deliverable and how stakeholders do benefit from those. Domains and stakeholders represent the common basis linking the work in this Deliverable to the effort done in WP1 and WP2, on one hand, and WP4 on the other hand. Thus, this Chapter summarises the CONCORDIA domains of interest as of defined in Deliverable D4.1 and secondly showing the mapped stakeholders. This information is used to support the purpose of this Deliverable. It is essential for consistency and readability purposes across the three consecutive Deliverables D4.1, D4.2, and D4.3. Therefore, this chapter at hand is extracted as such from Deliverable D4.1. A reader who already knows the domain of interests and stakeholders considered by CONCORDIA (as provided in the last deliverables) can go directly to Chapter 3 of this deliverable. Otherwise, it is strongly recommended to check the content available in this chapter.

### 2.1. Domains of Interest

Cybersecurity threats are analyzed in this deliverable from different perspectives, called domains, to identify emerging threats and attacks and set the scene for the associated implications in relation to the domains of interest of CONCORDIA. These domains, taken from the research domains of WP1 (*cf.* Figure 1), are: (i) Network-centric, (ii) System/Software-centric, (iii) Application/Data-centric, (iv) User-centric, (v) Internet-of-Things (IoT)/Device-centric security. Along the lines of the related discussion under D4.1, due to their importance, application- and data-centric security are treated separately in this deliverable as well.

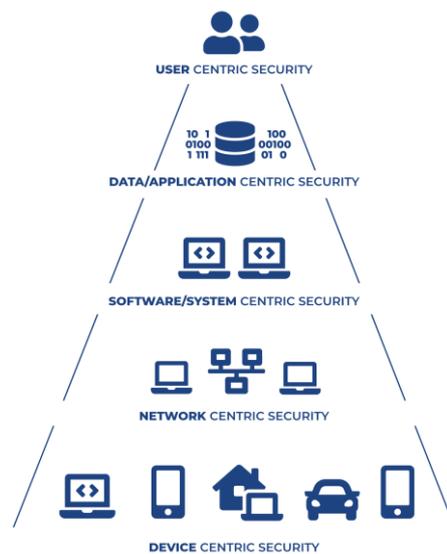


Figure 1: Domain of Interest

Note that the above domains depicted in Figure 1 apply to any environments ranging from traditional distributed Information Technology (IT) systems to devices that produce raw data, such as embedded systems, sensors, IoT devices, drones, and the associated security issues (*e.g.*, IoT security), via service-based systems, such as, service-oriented architecture, cloud, and micro-services.

## 2.2. Mapping of Stakeholders

The vision of CONCORDIA is to build strong cooperation between all its stakeholders and foster the development of IT products and solutions along the whole supply chain. Figure 2 shows the first step implemented [2] in identifying CONCORDIA stakeholders and the interaction between them. Several key stakeholders have been identified with which CONCORDIA will establish and foster liaisons. Stakeholders that could be the network members are European entities, Research entities, Companies, National and International entities [10]. The list of identified stakeholders is certainly not exhaustive and additional stakeholders can be identified.

The possible European entities can be the European Union Agency for Network and Information Security (ENISA), the Computer Emergency Response Team for the EU (European Union) Institutions, bodies and agencies (CERT-EU), European Strategic Intelligence and Security Center (ESISC), and European Cyber Security Organization (ECSO). These entities are the center of expertise for cybersecurity in Europe. Moreover, the stakeholders in Figure 2 also include national entities and national agencies. A few examples of the national agencies are the Global Cyber Security Center (GCSEC), the National Cyber Security Agency of France, and the National Cyber Security Centre of Lithuania. National agencies are responsible for developing and distributing awareness and knowledge on cybersecurity. They provide support to the national entities and companies on policies, regulations, and standards. National entities include the Military, Navy, Healthcare sector, and Airlines. In some cases, they manage national entities' Internet operations, propose cybersecurity plans, and investigate cybersecurity attacks.

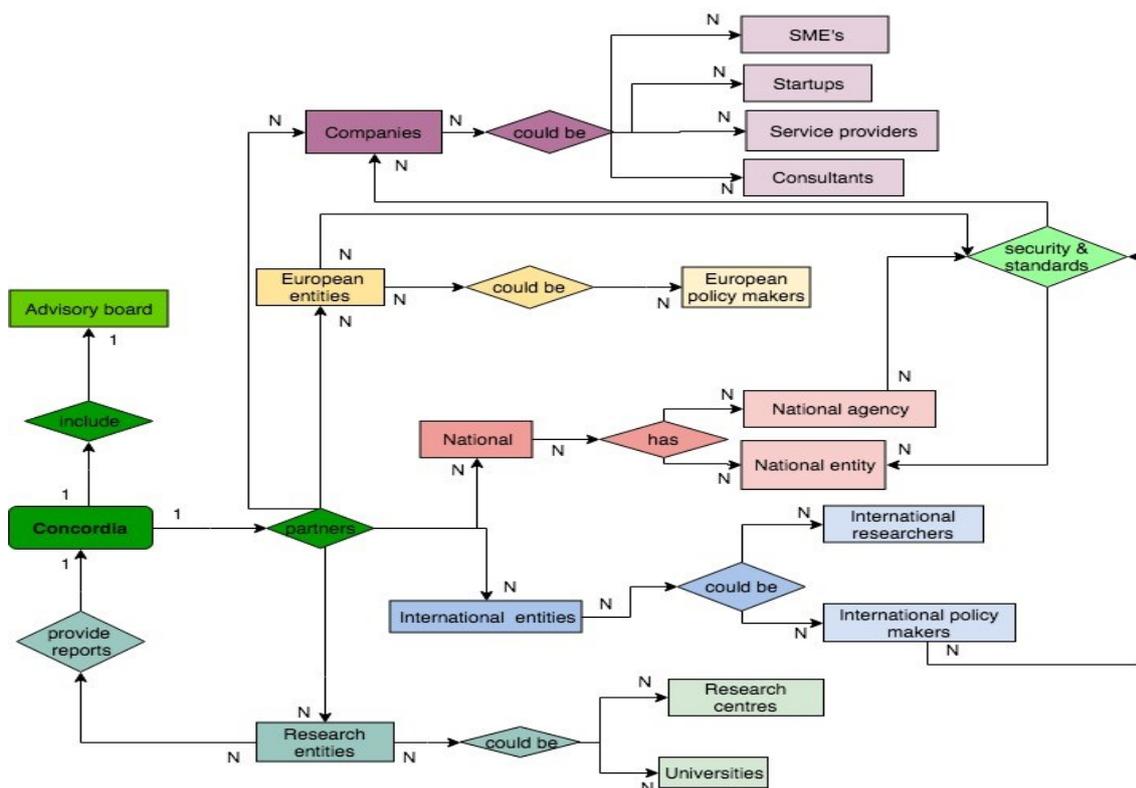


Figure 2: CONCORDIA Stakeholders [2]

### 3. Technical Perspectives: Cybersecurity Research Actions and Countermeasures

This chapter analyses and discusses research actions and countermeasures with reference to the threats and vulnerabilities in D4.1 and the technical gaps and challenges in D4.2, managing crosscutting aspects of the threat landscape affecting multiple domains of interest. In particular, WP4 revises the landscape proposed in D4.1 and D4.2 presenting new threats, gaps, and challenges emerged in the last year in the six domains of interest (Section 3.1). Relevant countermeasures and research actions in these six domains of interest are discussed in Section 3.2. Finally, a summary of and final remarks on the work done on technical aspects of cybersecurity is presented. Appendix A. Threats, Gaps, Challenges, Countermeasures, Research Actions: Summary, outlines the complete sets of threats, gaps, challenges, countermeasures, and research actions identified in D4.1, D4.2, D4.3, and their relationship. B. Mapping Between a Selection of Published Papers in WP1 and Gaps and Challenges in T4.1 maps different work published in the WP1 of CONCORDIA with gaps and challenges identified by T4.1 and described in this section.

#### 3.1. New Threats, Gaps, and Challenges

This section presents an update on threats, gaps, and challenges (for each domain of interest) with respect to the cybersecurity threat map in D4.2. A final summary of our findings with the complete lists of threats, gaps, and challenges is available in the Appendix A (at the end of this document). Also, examples of works addressing the different threats and gaps mapped are highlighted in the Appendix B.

##### 3.1.1. Device/IoT-Centric Security

New threats as determined include:

**T1.4.7 – Device hijacking.** An attacker can hijack and take control of a connected device without changing the basic functionality of the device and thus remain undetected. By hijacking a single device, the attacker can use it to infect the rest of the interconnected devices, such as smart meters in the grid. In the case of Industrial IoT (IIoT), by using compromised smart meters, a hijacker can launch ransomware attacks against Energy Management Systems (EMSs) and meddle with power lines.<sup>12</sup>

**T1.4.8 – Social engineering.** Social engineering attacks often do not take much effort to execute on IoT devices. Wearable devices collect a large amount of personal information for developing a personalized user experience. However, attackers can infiltrate such devices to obtain confidential information such as the users' bank details and home addresses. Exploiting this kind of information, attackers can unleash advanced social engineering attacks aimed at users and their family members through vulnerable IoT networks.<sup>13</sup>

New gaps and challenges:

**G1.12 – Gaps in insufficient data protection (communication and storage).** One of the main challenges for IoT privacy and security is that compromised devices can be used for

---

<sup>12</sup> Industrial IoT: Threats and Countermeasures, <https://www.rambus.com/iot/industrial-iot/>

<sup>13</sup> 8 TYPES OF INTERNET OF THINGS SECURITY THREATS, <https://www.bntimes.com/technology/8-types-of-internet-of-things-security-threats>

unauthorized access to confidential data. To prevent hackers from accessing IoT networks, secure data storage and network segregation are of utmost importance. Data encryption can be used to prevent data visibility in the case of unauthorized access, hence minimizing the risk of data theft. Moreover, data encryption is also efficient in preventing attacks such as eavesdropping and man-in-the-middle.<sup>14</sup>

**G1.13 – Gaps in device management and the use of outdated components.** A study on the Internet of Medical Things (IoMT) published in July 2020 unveiled a significant number of vulnerabilities across different connected objects. It was found out, that 51% of consumers were unaware of smart objects that were used, while 75% of devices violated VLAN, and 86% of healthcare deployments used recalled devices.<sup>15</sup> As a result, the healthcare industry found itself under the increased risk of ransomware attacks, which took advantage of the mix of legacy systems and connected devices, in order to disrupt operations, compromise customer data, and inflict reputational damage. Additionally, as the survey revealed, the use of deprecated software components, operating systems, and third-party software of hardware components could lead to compromised smart devices.<sup>16</sup>

### 3.1.2. Network-Centric Security

New threats as determined include:

**Threat T2.1.2: Security misconfigurations in systems/networks.** Security misconfiguration is possible to occur at any level including poorly configured APIs, network functions, access control rules, network slices, administration rights, virtualized environments, traffic isolation, edge nodes, orchestration software and firewalls. The exploitation of a misconfigured system creates the opportunity for a threat actor to reach critical assets in the network.

**Threat 2.3.7: Exploitation of system administration tools and fileless malware.** Fileless malware is designed to bypass familiar detection controls and infiltrate key systems by ‘living off the land’, using approved platforms or software tools that already exist within corporate networks. This approach allows attackers to get around common detection methods that scan for malicious file attachments and, at the same time, not to have to design their own attack framework - as they use existing system tools decreasing the time required for malware development. It is expected that attackers will use fileless malware to compromise service network providers rather than specific groups and then to use their existing infrastructure to attack downstream clients. A study conducted by Positive technologies shows that more than 50% of threat groups leverage publicly available penetration testing and system administration tools to develop attack strategies. The exploitation of system administration and penetration tools, like Cobalt Strike, PowerShell Empire and BloodHound, is increasing. Cybercriminals are using these and other legitimate admin tools, to carry out and hide their activities, a tactic known as ‘living off the land’. By making use of legitimate admin tools that are already installed on target computers and running scripts and shell code directly in memory, attackers can greatly reduce the chances of being detected, as the attack creates fewer new files, that antivirus and other detection tools can spot. The result is that these attacks generally go undetected.

---

<sup>14</sup> IOT SECURITY ISSUES IN 2021: A BUSINESS PERSPECTIVE,

<https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats>

<sup>15</sup> Threat highlight: Analysis of 5+ million unmanaged, IoT, and IoMT devices,

<https://www.helpnetsecurity.com/2020/07/24/analysis-of-5-million-unmanaged-iot-and-iomt-devices/>

<sup>16</sup> THE TOP 1- IOT SECURITY THREATS AND VULNERABILITIES, IOT SECURITY ISSUES IN 2021: A BUSINESS PERSPECTIVE, <https://blog.particle.io/the-top-10-iot-security-threats/>

**Threat T2.3.8: Exploitation of Application Programming Interfaces (APIs).** The adoption of Application Programming Interfaces (APIs) has been increased, during the last years, because of their use in 5G networks. The shift to service-based interfaces within the 5G core and the increased use of API-based communication exposed to external networks, introduce a new attack surface. A poorly designed or configured API, with inaccurate access control rules may expose core network functions and sensitive parameters. The exploitation can target different types of API, related to internal network functions, internetworking interfaces, roaming interfaces, and the like, which are exposed in different layers of the network.

New gaps and challenges include:

**G2.14 - Gaps on ‘Defense in Depth’.** ‘Defense-in-depth’ is about being able to detect and stop what the first line of defense lets through. One of the most relevant gaps in ‘Defense-in-depth’, is to detect attacks, that the network firewalls have not blocked, for example due to a misconfiguration –and– and/or that network IDS or antivirus have to let pass - for example because attackers have found a way to bypass signature-based detection. Intruders are using the land of land attacks, to get into the networks’ systems via trusted programs that are not going to arouse any suspicions. With this tactic, intruders can get around traditional protection systems, which will not be triggered by the unusual use of apparently secure software. It also allows cybercriminals to get onto IT systems securely, and even spend several months inside without setting off any kind of alarm. Given the circumstances, it is also much harder to identify where the attack comes from, compared to when certain files are used. The reason for this is that the vast majority of cybersecurity solutions are unable to detect dangerous behavior, when it is carried out, using tools classified as legitimate. For these reasons, it is necessary to identify and enable new methods for security monitoring, response, and recovery against the existing security solutions such as blacklisting/whitelisting, antivirus-like approaches, and anomaly detection.

**G2.15 - Gaps on attack surface awareness.** Knowing the network attack surface is very complex and requests a lot of time since it includes visibility on all the networks’ systems where unauthorized users or attackers can exploit vulnerabilities to gain access to systems and stage an attack. One of the main gaps is related to this visibility on the network that, in most cases, is partial and changing over time as new technologies, users, and connections are introduced, expanding the network threat surface and increasing the number of attackable points and the overall risk. The human factor is also a growing concern, especially considering the increasing number of remote workers due to the COVID-19 pandemic. To secure remote workers, additional technologies and tools have been adopted, however, in parallel new tools need to be securely integrated into a tech stack. Misconfigured software or technology can introduce security gaps, exposing the users to new threats. These aspects imply that networks and systems are becoming more complex, increasing the threat surface, thus making it harder to spot attacks early and to take appropriate action to mitigate cyber threats.

**G2.16 - Security of the new Open Radio Access Network model.** Open RAN is an emerging model to build the RAN for mobile operators.<sup>17</sup> The new model is attractive to the operators because it permits the reduction of both CAPEX and OPEX, by adopting open hardware and open software; at the same time, it breaks the traditional vendor lock-in in favour of true market competition. However, there are challenges associated with the new model that still have to be better identified and correctly managed. From the security point

---

<sup>17</sup> O-RAN ALLIANCE is Transforming the Radio Access Network Industry Towards Open, Intelligent, Virtualized and Fully Operable RAN, <https://www.o-ran.org/>  
www.concordia-h2020.eu

of view, the multi-vendor environment will increase the threat surface, especially because new software, new interfaces, new protocols will be deployed in the field, in particular for the 5G. Moreover, new emerging vendors, with little or no experience, will enter the market.

**G2.17 - Gaps in the security of network slicing.** Network slicing sets up several vulnerabilities that security mechanisms designed into 5G's Service Based Architecture are not currently resourced to detect and protect against. Current security mechanisms in 5G architectures are focused on detecting and protecting against malicious User Equipment (UE), but less so in filtering signaling between and within Network functions and slices themselves. The underlying problem is that no layer matching is mandated by the specifications. Recent research<sup>18</sup> examined 5G core networks that contain both shared and dedicated network functions, is revealing that when a network has these 'hybrid' network functions, that support several slices, there is a lack of mapping between the application and transport layers identities. This is a relevant gap since i) operators will share network functions between slices and ii) slices may also need to communicate with each other. This flaw in the industry standards has the impact of creating an opportunity for an attacker to access data and launch denial of service attacks across multiple slices if they have access to the 5G Service Based Architecture. For example, a hacker comprising an edge network function connected to the operator's service-based architecture could exploit this flaw in the design of network slicing standards to have access to both the operator's core network and the network slices for other enterprises.

### 3.1.3. System-Centric Security

New threats as determined include:

**T3.4.9 – State-sponsored attacks.** Cyberattacks are increasingly harmful and closely resemble the tactics used by nation-states. Attackers increasingly aim to destroy a target system, for instance implementing nefarious DDoS attacks (threat T3.4.2),<sup>19</sup> to make it unusable and, possibly, unrecoverable.<sup>20</sup> These attacks are getting more complex and larger than ever<sup>21</sup> and are often coupled with extortion attacks (see T4.4.9).

New gaps and challenges include:

**G3.24 - Gaps in the configuration of cloud storage.** Security issues in cloud computing occur as a result of oversights and superficial audits. This makes cloud servers vulnerable to breaches. Types of misconfiguration include using default cloud security settings of the server, mismatched access management that causes an unauthorized person to get access to the sensitive data, and garbled data access in which confidential data is left open to

---

<sup>18</sup> 'Major' security flaw detected in 5G core network slicing design, <https://www.computerweekly.com/news/252498422/Major-security-flaw-detected-in-5G-core-network-slicing-design>

<sup>19</sup> ENISA. ENISA Threat Landscape 2021 – April 2020 to mid-July 2021. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>

<sup>20</sup> VMware. Shields Up: Prepare for Destructive Cyberattacks. 2022. <https://blogs.vmware.com/security/2022/03/shields-up-prepare-for-destructive-cyberattacks.html>

<sup>21</sup> David Warburton, 2022 Application Protection Report: DDoS Attack Trends, March 2022, <https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends>

everyone.<sup>22</sup> In 2017, misconfiguration of the AWS server left the top-secret army and NSA data publicly accessible by anyone.<sup>23</sup>

### 3.1.4. Data-Centric Security

New threats as determined include:

**T4.4.8 – Data extraction from ML models.** Machine Learning (ML) models can be attacked at any phase of their life cycle. Poisoning attacks (threats T4.3.1 and T4.3.2) are increasingly used to attack the ML training phase. Membership inference attacks aim to recover the training set from a deployed ML model. A pioneering work in 2017 permitted to infer the presence of a data point in the training set based on model predictions only.<sup>24</sup> This attack has been later demonstrated on very large models<sup>25</sup> and poses a significant privacy (and economic) risk.

**T4.4.9 – Extortion attacks.** Shift in ransomware-based attacks point to the so-called *double-extortion strategy*. First, attackers gain access to the system encrypting data with the ransomware. Second, attackers exfiltrate (sensitive) data, threatening the target victim with the sale or dissemination of data if a ransom is not paid.<sup>26</sup> This is a double extortion because the victim must pay *i)* to have the ransom removed and *ii)* by a certain deadline to avoid data publication.<sup>27</sup> As a consequence of double-extortion attacks, backups become less effective in protecting against ransomware.

New gaps and challenges include:

**G4.10 - Gaps in the distributed data and frameworks.** Analyzing big data requires organizations to spread it over multiple systems, which is usually done with Hadoop. However, accomplishing security requirements in Hadoop is a challenging task, which reflects in, difficulties in detecting data breach when it occurs. Moreover, attackers can render MapReduce useless by displaying incorrect lists of values and key pairs.<sup>28,29,30</sup>

**G4.11 - Gaps in the use of non-relational databases.** Since relational databases sometimes have difficulties handling big data due to the scalable and diverse nature of big data, non-relational databases (NoSQL) are often the solution for handling big data. Despite overcoming some shortcomings of the relational databases by providing more flexibility

---

<sup>22</sup> CLOUD COMPUTING SECURITY RISKS IN 2021, AND HOW TO AVOID THEM, <https://theappsolutions.com/blog/development/cloud-security-risks/>

<sup>23</sup> TOP secret Army, NSA data found on public internet due to misconfigured AWS server, <https://www.cyberscoop.com/nsa-army-leak-red-disk-aws-upguard-chris-vickery/>

<sup>24</sup> R. Shokri, M. Stronati, C. Song, V. Shmatikov. “Membership Inference Attacks Against Machine Learning Models”, in Proc. of IEEE S&P 2017, San Jose, CA, USA, May 2017.

<sup>25</sup> N. Carlini, F. Tramèr, E. Wallace, M. Jagielski, A. Herbert-Voss, K. Lee, A. Roberts, T. Brown, D. Song, Ú. Erlingsson, A. Oprea, C. Raffel. “Extracting Training Data from Large Language Models”, in Proc. of USENIX 2021, Virtual, August 2021.

<sup>26</sup> TrendMicro. Toward A New Momentum. Trend Micro Security Predictions for 2022.

<sup>27</sup> ZDNet. Black Hat: Enterprise players face ‘one-two-punch’ extortion in ransomware attacks. 2021. <https://www.zdnet.com/article/black-hat-enterprise-players-face-one-two-punch-extortion-tactics-in-ransomware-attacks/>

<sup>28</sup> 6 Big Data Security Issues for 2019 and Beyond, <https://rtslabs.com/6-big-data-security-issues-for-2019-and-beyond/>

<sup>29</sup> 9 Key Big Data Security Issues, <https://cybersecurity.att.com/blogs/security-essentials/9-key-big-data-security-issues>

<sup>30</sup> Big Data Security: Challenges and Solutions, <https://www.dataversity.net/big-data-security-challenges-and-solutions/#>

and scalability, NoSQL databases lack the security that is inherent in relational databases. Mitigating the lack of security in NoSQL databases requires additional workarounds, such as using middleware or setting the database in a trusted environment with additional security options, which is often not simple to accomplish.<sup>28</sup>

### 3.1.5. Application-Centric Security

New threats as determined include:

**T5.3.7 – Virtualization.** Virtualization is used to consolidate physical machines, allowing many applications, or even operating systems, to coexist in an isolated way on the same host. Since virtualization is often used for multitenancy, it opens to new threats specifically aimed to exploit this aspect, gaining, for instance, access to other tenant's data. At the same time, a threat affecting the underlying virtualization technology can have a great impact on the overall system security. Within this context, hardware vulnerabilities such as *Meltdown* and *Spectre* have gained high visibility. Finally, the situation can be further exacerbated by new lightweight virtualization technologies based on a less strict isolation.

**T5.3.8 – Source code breach.** Also known as reverse engineering, it attempts to recover the source code of an application from its executable code.<sup>31</sup> It also applies to ML models, with model stealing attacks aiming to recover a trained model. Preliminary approaches to tackle this threat include methods to determine whether a model is the result of a recovering process.<sup>32</sup> This threat is dangerous in itself, while it can also serve as a preparatory step for other attacks (e.g., to collect information about the implemented security measures or as a basis to membership inference attacks in T.4.4.8).

No new gaps and challenges had been identified.

### 3.1.6. User-Centric Security

New threats include:

**T6.5.3 - Pivoting.** Attackers use a pivoting approach when they leverage the capabilities of a compromised user to attack other users or an organization. The attack may be accomplished without the “pivot” users' knowledge (*i.e.*, by using involuntarily leaked access information) or by extortion (*i.e.*, through blackmailing). In both cases, the compromised users are a threat with, potentially, comparable capabilities to a malicious insider.

New gaps and challenges include:

**G6.6 - Gaps on protection from online scammers.** With the emergence of COVID-19, the notorious FUD triple (fear, uncertainty, and doubt) has resurfaced in society. Similarly, as in the previous states of distress, the scammers are again ready to exploit distraught, desperate, and depressive people. During the course of the pandemic, cybercriminals have

---

<sup>31</sup> OWASP. Reverse Engineering and Code Modification Prevention. [https://owasp.org/www-project-reverse-engineering-and-code-modification-prevention/migrated\\_content](https://owasp.org/www-project-reverse-engineering-and-code-modification-prevention/migrated_content)

<sup>32</sup> P. Maini, M. Yaghini, N. Papernot. “Dataset Inference: Ownership Resolution in Machine Learning”. In Proc. of ICLR 2021, Vienna, Austria (Virtual), May 2021.

carried out a wide range of well-known online scams, including phishing email campaigns, fake products, fraudulent advertising, and preposterous pseudoscientific theories.

## 3.2. Countermeasures and Research Actions

This section presents an overview of countermeasures addressing identified threats, and research actions aimed to fill gaps and challenges (for each domain of interest). A complete summary of our findings with the complete list of countermeasures and research actions mapped on threats, gaps, and challenges is presented in Appendix A.

### 3.2.1. Device/IoT-Centric Security

Based on the discussion of respective countermeasures identified regarding Device/IoT-Centric Security, these are briefly evaluated and complemented with a description of research actions foreseen.

#### 3.2.1.1. Countermeasures

We provide an overview of existing countermeasures that focus on one or more threats, and address gaps and challenges in Appendix A.1. This section aims to present the status of cybersecurity solutions connecting them to identified threats and gaps. We discuss classes of countermeasures, each describing the most relevant solutions to date.

**C1.1 - Performing contextual vulnerability assessment.** IoT devices have to be constantly monitored throughout their lifecycle to track potential vulnerabilities from inside the devices. Moreover, manufacturers should ensure that devices ship without vulnerabilities and are resistant to attacks by releasing timely critical updates and by monitoring devices for indications of possible software failures or other critical situations<sup>33</sup>.

**Threats:** T1.3.3 - Lack of control on safety implications — COVID-19, T1.4.2 - Denial of service, T1.4.3 - Malicious code/software/activity, T1.4.6 - Code execution and injection (unsecured APIs)

**Gaps:** G1.1 - Gaps in design, G1.4 - Gaps on diagnosis and response capabilities, G1.9 - Product lifecycle management leakages, G1.11 - Gaps in handling critical scenarios, G1.13 - Gaps in device management and the use of outdated components

**C1.2 - Implementing segmentation.** Segmentation can be done to increase data and network security in IoT devices and prevent attackers from traversing components laterally and thus infecting other components. It is a technique that isolates specific components and ensures the use of different layers of security measures for protecting sensitive data. The first step of the segmentation is to create a list of connected IoT devices, their respective connection methods, type of data transmitted, and to which other device each device connects. Devices that do not have access network should be disabled. During the segmentation process, it is advisable to segment IoT devices by category, including infrastructural, data-collecting, or user endpoints<sup>34</sup>. Afterward, network policies for thwarting unauthorized access should be assigned as per the requirements of each endpoint's purpose<sup>35</sup>.

<sup>33</sup> AN "INSIDE-OUT" APPROACH IS NECESSARY TO DETECT AND MITIGATE IOT BREACHES, <https://www.cybeats.com/blog/an-inside-out-approach-is-necessary-to-detect-and-mitigate-iot-breaches>

<sup>34</sup> HOW TO MITIGATE IOT SECURITY THREATS IN 2021, <https://mobidev.biz/blog/mitigate-internet-of-things-iot-security-threats>

<sup>35</sup> TOP IOT THREATS AND HOW TO AVOID THE NEXT BIG BREACH, <https://www.cybeats.com/blog/top-iot-threats-and-how-to-avoid-the-next-big-breach>

**Threats:** T1.1.1 - Information leakage/sharing due to human errors, T1.2.1 - Interception of information, T1.2.2 - Unauthorized acquisition of information (data breach), T1.3.2 - Extraction of private information, T1.3.3 - Lack of control on safety implications - COVID-19, T1.4.3 - Malicious code/software /activity, T1.4.7 – Device hijacking

**Gaps:** G1.2 - Gaps on protection mechanisms adoption and hardening, G1.12 - Gaps in insufficient data protection (communication and storage), G1.13 - Gaps in device management and the use of outdated components

**C1.3 - Ensuring device authentication.** Establishing necessary authentication measures, such as biometrics, multi-factor authentication, and digital certificates can ensure the protection of IoT endpoints<sup>34</sup>. All interconnected devices should be secured by full authentication and factory default passwords should be changed. Moreover, to enforce mutual authentication between devices and services, lightweight cryptography symmetric and asymmetric key algorithms, such as the Secure Hash Algorithm (SHA-x) along with hash-based message authenticated code (HMAC) and Elliptic Curve Digital Signature Algorithm (ECDSA) can be deployed<sup>12</sup>. User data and communication streams from the sensors, have to be encrypted, to ensure their integrity by using hash integrity checkers and authentication methods that enable communication only between trusted entities<sup>36</sup>.

**Threats:** T1.2.1 - Interception of information, T1.2.2 - Unauthorized acquisition of information (data breach), T1.3.2 - Extraction of private information, T1.4.1 - Identity fraud, T1.4.7 – Device hijacking

**Gaps:** G1.3 - Gaps on authorization and authentication, G1.12 - Gaps in insufficient data protection (communication and storage)

**C1.4 - Deploying Public Key Infrastructure (PKI).** A Public Key Infrastructure (PKI) utilizes a combination of encryption, authorization, authentication, and Intrusion detection mechanisms. It can be implemented in the recognition layer of IoT architecture. PKI is based on an RSA encryption algorithm as the public and private keys, in which the private key is stored at the base station and the public key is distributed to each connected node [13]. This way, security is ensured in each interconnected node. Furthermore, end-users can customize PKI systems according to their specifications to improve threats detection and thus fulfil the cybersecurity goals<sup>37</sup>.

**Threats:** T1.2.1 - Interception of information, T1.2.2 - Unauthorized acquisition of information (data breach), T1.3.2 - Extraction of private information, T1.4.7 – Device hijacking

**Gaps:** G1.2 - Gaps on protection mechanisms adoption and hardening, G1.3 - Gaps on authorization and authentication, G1.11 - Gaps in handling critical scenarios

**C1.5 - Deploying AI and machine learning.** AI-based Intrusion Detection Systems (IDS) are one of the novel solutions for monitoring the network, collecting and analyzing information from previous attacks. These systems can predict incoming attacks based on historical data and suggest ways to mitigate them. Through real-time ML algorithms, these systems can even predict never before seen attacks that are based on some previous attacks. ML-based IDS systems can be categorized into two broad categories, namely anomaly IDS and misuse or signature IDS. The first can detect the attacks by comparing the current real-time traffic with the previous normal levels of real-time traffic. The latter one compares the current real-time traffic with the known patterns of various previous attacks. Moreover, other ML algorithms such as Linear Discriminant Analysis (LDA), Classification and

---

<sup>36</sup> Bock, L.; “The Internet of 12 Things Operate on a Cowboy Code—There Are No Rules,” LinkedIn, 18 June 2017, <https://www.linkedin.com/pulse/security-privacy-iot-lisa-bock/>

<sup>37</sup> IOT SECURITY: UNDERSTANDING THE DANGERS AND MITIGATING THREATS, <https://www.analyticsinsight.net/iot-security-understanding-the-dangers-and-mitigating-threats/>

Regression Trees (CART), and Random Forest are also efficient for attack identification and classification<sup>34</sup>.

**Threats:** T1.4.2 - Denial of service, T1.4.3 - Malicious code/software/activity, T1.4.6 - Code execution and injection (unsecured APIs)

**Gaps:** G1.4 - Gaps on diagnosis and response capabilities, G1.11 - Gaps in handling critical scenarios

**C1.6 - Utilizing security analytics, monitoring, and risk assessment techniques.** To ensure that interconnected IoT devices communicate regularly, organizations and end-users have to embrace a number of the available risk assessment tools, techniques, and strategies [14]. Device monitoring tools are highly useful in identifying and tracking suspicious activities and performing risk assessments. Moreover, security monitoring tools can be used to capture data about the overall state of all IoT devices and traffic between them and to use it to identify possible security violations and system threats. Afterward, actions in the context of security policies, such as device revocation and IoT device isolation can be enforced<sup>12</sup>. Another useful means of identifying suspicious events and responding to threats is through the use of IoT security analytics. They can be used for collecting, correlating, and analyzing the data, which can be then used for visualization of IoT activities. Both IoT gateways and sensor CPU activity should also be monitored and obtained data should be combined to ensure only approved activities can ensue<sup>35</sup>.

**Threats:** T1.3.3 - Lack of control on safety implications - COVID-19, T1.4.3 - Malicious code/software/activity, T1.4.6 - Code execution and injection (unsecured APIs)

**Gaps:** G1.2 - Gaps on protection mechanisms adoption and hardening, G1.4 - Gaps on diagnosis and response capabilities

**C1.7 - Utilizing SDN with IoT.** One of the trending network security management approaches in different areas, including smart homes and e-health systems, is software-defined networking. It consists of two separated planes, namely the control and the data plane, which execute in the hardware and the software respectively. SDN can be used for monitoring the traffic and detecting malicious activities by identifying and isolating the compromised nodes from the network [13].

**Threats:** T1.4.2 - Denial of service, T1.4.3 - Malicious code/software/activity, T1.4.6 - Code execution and injection (unsecured APIs), T1.4.7 – Device hijacking

**Gaps:** G1.2 - Gaps on protection mechanisms adoption and hardening, G1.4 - Gaps on diagnosis and response capabilities

**C1.8 - Testing.** Proper testing assures that the IoT devices and related protocols can cope with the IoT ecosystem by defining market-accepted test specifications, which in turn helps to accept devices that cooperate with IoT objects. To harden the security configurations, IoT web interface management should be tested, while physical ports and authentication and interaction between devices and the cloud should be assessed<sup>38</sup>.

**Threats:** T1.1.2 - Inadequate design and planning or incorrect adaptation, T1.1.3 - Inadequate design and planning or incorrect adaptation in the critical scenario - COVID-19, T1.4.2 - Denial of service

**Gaps:** G1.1 - Gaps in design, G1.2 - Gaps on protection mechanisms adoption and hardening, G1.3 - Gaps on authorization and authentication, G1.7 - Lack of security-dedicated budget

**C1.9 - Fostering security-by-design approach.** All personnel involved in the design and development of IoT devices should pay attention to security fundamentals and collaborate to accomplish security-by-design. Security features, such as firewalls, tamper detection

---

<sup>38</sup> Security Issues in IoT: Challenges and Countermeasures, <https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/security-issues-in-iot-challenges-and-countermeasures>

capabilities, and encryption capabilities should be added in the design phase of IoT devices. Security-by-design should be an integral part of the entire ecosystem that is running IoT devices and services<sup>39</sup>. In addition, the CIA triad (Confidentiality, Integrity, and Availability) should be the primary goal for IoT vendors. Lastly, manufacturers should treat IoT devices as any other traditional devices they produce.

**Threats:** T1.1.2 - Inadequate design and planning or incorrect adaptation, T1.1.3 - Inadequate design and planning or incorrect adaptation in the critical scenario – COVID-19, T1.4.4 - Misuse of assurance tools, T1.4.5 - Failures of business process

**Gaps:** G1.1 - Gaps in design, G1.7 - Lack of security-dedicated budget

**C1.10 - Raising security awareness.** One of the most important security measures for ensuring the success and growth of IoT frameworks is raising security awareness among participating users [15]. The study conducted by Patton et al. [16] showed that a large number of IoT devices, including web cameras, traffic control devices, and printers are either not using passwords or using default passwords, hence making them easily accessible. Continuing the same practice would render IoT devices to cause more harm than good. Therefore, security awareness campaigns and proper training can aid in mitigating the aforementioned issues.

**Threats:** T1.1.1 - Information leakage/sharing due to human errors, T1.3.3 - Lack of control on safety implications - COVID-19, T1.4.5 - Failures of business process, T1.4.8 - Social engineering, T1.5.1 - Violation of laws or regulations, T1.6.2 - Lack of strong cyber hygiene practices – COVID-19

**Gaps:** G1.5 - Lack of awareness and knowledge (skill shortage), G1.10 - Gaps in cyber hygiene practices

**C1.11 - Firmware maintenance and integrity.** Regular firmware updates and maintenance are essential for safeguarding the IoT ecosystem and handling functional operations. Maintenance interfaces should have access to the application runtime environment and security settings, hence enabling IoT firmware and OS updates<sup>38</sup>. To prevent attacks targeting firmware, the secure boot has to be used to ensure that a device can only execute OEM or trusted party code. IoT devices should only be able to communicate with authorized services to avoid the risks of being targeted by malicious activities<sup>12</sup>.

**Threats:** T1.3.1 - Device modification, T1.4.6 - Code execution and injection (unsecured APIs), T1.4.7 - Device hijacking

**Gaps:** G1.2 - Gaps on protection mechanisms adoption and hardening, G1.6 - Lack of interoperability, G1.9 - Product lifecycle management leakages, G1.11 - Gaps in handling critical scenarios, G1.12 - Gaps in insufficient data protection (communication, storage)

**C1.12 - Enforcing regulations.** More regulations are necessary to ensure that manufacturers and vendors prioritize security and provide guidelines on IoT developers' expectations, and thus providing the necessary level of transparency to the end-users. Policies such as IoT Cybersecurity Improvement Act 2020<sup>40</sup> and the EU General Data Protection Regulation (GDPR)<sup>41</sup> should be enacted across the global level. The act is aimed at federal agencies, and it obliges the National Institute of Standards and Technology (NIST) to develop IoT guidelines, while the GDPR introduced mandatory notification schema

<sup>39</sup> White Hat Security, "IoT Security—Combining Innovation With Protection," <https://www.whitehatsec.com/trending/content/iot-security-combining-innovation-protection>

<sup>40</sup> Cybersecurity Improvement Act signed into law inching IoT toward more robust security, <https://www.securityinfowatch.com/cybersecurity/article/21203756/cybersecurity-improvement-act-signed-into-law-inching-iot-toward-more-robust-security>

<sup>41</sup> Chapin, M., et al; *Implication of the General Data Protection Regulation*, March 2018, [https://www.aacrao.org/docs/default-source/signature-initiative-docs/gdpr/gdpr\\_discussiondraft\\_03272018\\_v2.pdf?sfvrsn=4556dd66\\_0](https://www.aacrao.org/docs/default-source/signature-initiative-docs/gdpr/gdpr_discussiondraft_03272018_v2.pdf?sfvrsn=4556dd66_0)

which coerces data controllers to report data breaches on time. Moreover, GDPR ensures that data controllers address data breaches according to the provided guidelines<sup>42</sup>.

**Threats:** T1.3.3 - Lack of control on safety implications – COVID-19, T1.6.1 - Skill shortage, T1.4.4 - Misuse of assurance tools

**Gaps:** G1.6 - Lack of interoperability, G1.8 - Fragmentation in security approaches and regulations

### Highlights on Identified Countermeasures

Before the shipment, manufacturers must ensure that the IoT devices are robust to known attacks by releasing timely patches and analyzing critical situations. Segmentation, that is, isolating components by different categories can prevent attackers from spreading infections to other IoT components. Due to the resource-constrained nature of the IoT devices, developers should focus on ensuring mutual authentication through lightweight cryptographic algorithms, such as SHA-x, HMAC, and ECDSA. Detecting and thwarting malicious activities and attacks, calls for the deployment of novel technologies, including AI and ML-based IDSs, as well as taking advantage of IoT security analytics, monitoring, and risk assessment techniques. In addition, SDN can also be used for monitoring the traffic between IoT nodes and isolating compromised nodes from the network. IoT firmware can be protected from incoming attacks through regular maintenance and updates. Additionally, IoT devices should only be allowed to communicate with authorized services to thwart potential malicious activities. More IoT-specific regulations and policies, such as IoT Cybersecurity Improvement Act 2020 are necessary to provide guidelines for IoT developers and ensure transparency for end-users.

#### 3.2.1.2. Research Actions

The following discussion addresses relevant research actions that need to be taken to mitigate threats, gaps, and challenges identified above and reported in Appendix A.1.

**RA1.1 - ML/DL-based solutions.** Machine Learning (ML) and Deep Learning (DL) techniques can be used for tackling security issues in IoT devices by providing embedded intelligence. The reason behind this, lies in the fact that IoT networks generate vast amounts of real-time data that can be utilized by ML and DL techniques to offer insights and aid in decision-making. Among many other uses, ML and DL have the potential of leveraging privacy and access control issues, as well as reinforcing capabilities of attack detection, intrusion detection, malicious code identification, and malware analysis capabilities in IoT environments. There has been already significant work research done in all of the aforementioned areas, with significant caveats remaining to be solved. For attack detection, Rathore and Park [17] proposed a semi-supervised scheme based on Extreme Learning Machine (ELM) that relies on Fuzzy C-Means (FCM), while DL-based attack detection systems based on fog architecture were promoted in the works of Diro and Chilamkurti [18] and Abeshu and Chilamkurti [19]. SVM showed to be the best performing ML algorithm in detecting DoS attacks, as shown in the number of research endeavours [20] [21] [22]. ML and DL neural network algorithms such as ANN [23], RNN [24] [25], and Random Neural Networks (RaNN) [26] have been commonly experimented on for intrusion detection. Lastly, algorithms including SVM, PCA, RNN, as well as some novel algorithms, such as Learning-based Deep Q Network (LDQN) [27] have been used in an attempt to identify

---

<sup>42</sup> Bird & Bird, “Personal data Breaches and Notification,” <https://www.twobirds.com/~media/pdfs/gdpr-pdfs/42--guide-to-the-gdpr--personal-data-breaches-and-notification.pdf?la=en>

malicious activities affecting IoT. However, ML and DL come with significant bottlenecks that still need to be addressed. Choosing the most suitable model and labelling the training data remain cumbersome tasks to accomplish, while performance overhead, remains an issue due to the resource-constrained nature of the IoT devices. Moreover, anomalies created by various ML and DL algorithms pose an issue for critical infrastructure and real-time applications. When it comes to large IoT ecosystems, consisting of a multitude of different devices, more advanced ML capabilities that could grant stronger security features are necessary. Other challenges that require significant effort include scarcity of training datasets publicly available, imbalanced data in the time that attacks take place, merging available public datasets, and legislative challenges related to validation and certification of different IoT components and varying GDPR regulations. To solve the existing issues of ML approaches for securing IoT, more research endeavour is required on strengthening DL and Deep Reinforcement Learning (DRL) definitions to bolster their performances in terms of computational complexity, efficiency, and parameter tuning. Besides that, more novel hybrid learning techniques and data visualization techniques are still required for better data interpretation [28].

**Threats:** T1.1.3 - Inadequate design and planning or incorrect adaptation in the critical scenario - COVID-19, T1.2.1 - Interception of information, T1.2.2 - Unauthorized acquisition of information (data breach), T1.3.1 - Device modification, T1.3.2 - Extraction of private information, T1.3.3 - Lack of control on safety implications - COVID-19, T1.4.1 - Identity fraud, T1.4.2 - Denial of service, T1.4.3 - Malicious code/software/activity, T1.4.4 - Misuse of assurance tools, T1.4.5 - Failures of business process, T1.4.6 - Code execution and injection (unsecured APIs)

**Gaps:** G1.4 - Gaps on diagnosis and response capabilities, G1.9 - Product lifecycle management leakages, G1.11 - Gaps in handling critical scenarios, G1.13 – Gaps in device management and the use of outdated components

**RA1.2 - Blockchain-based solution.** Currently, IoT devices experience an ununiformed and inconsistent data flow as a result of both conflicting protocols and unstandardized designs. Updates to IoT devices are also non-compliant, making IoT devices entail constant maintenance. The reason is that the majority of the IoT vendors do not follow any access control or configurations standards, but rather create their proprietary ecosystems. Moreover, IoT infrastructure is centralized and utilizes a client/server model, rendering connected devices to be vulnerable to a wide array of potential attacks. Even though centralized infrastructure works considerably well in small-scale ecosystems, it is not suitable for large-scale projects. Hence, there is an increasing need to conduct research on the ways that decentralized solutions, particularly blockchain technology, could be incorporated in the IoT environment. The benefits of the blockchain, including its immutability, verifiability, and efficiency could help in overcoming current IoT issues. In other words, blockchain-based solutions could keep an immutable record of IoT devices and improve their security properties through the use of smart contracts. So far, blockchain-based solutions for IoT security have been taken under consideration in several works, but there is still room for improvement. One of the first such endeavours, has been carried out by the H2020 project “Secure and Safe Internet of Things” (SerIoT) to optimize the IoT platforms’ and networks’ security through the combination of blockchain technology, fog computing, honeypots, and SDN routers [29]. It considers a holistic approach to defining an end-to-end IoT network ecosystem with a multi-layered schema for different IoT layers. Their ultimate plan is to deploy their technology into IoT applications, to accomplish horizontal IoT and end-to-end security in IoT platforms, throughout Europe. To achieve secure mutual authentication and grant auditability and confidentiality, Lin et al. [30] proposed a blockchain-based system for enforcing fine-grained access policies. The authors combined blockchain with other technologies including MAC, ABS, and CL-

MRE to achieve high resilience against DoS, replay, MiTM, impersonation, and modification attacks. However, the proposed model remains an idea and requires further optimization and implementation in the real-world setting. More recently, in 2020, Mohanty et al. [31] proposed a Lightweight integrated Blockchain (ELIB) model and deployed it in a smart home environment. Their model consists of three optimizations, namely lightweight consensus algorithm, certificateless cryptography, and Distributed Throughput Management (DTM) scheme. This model also still has to be optimized from the energy consumption standpoint and yet has to be deployed on a wider scale. On the other hand, Singh et al. [32] proposed a Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence (BlockIoTIntelligence) system for IoT applications and techniques to support big data analysis. Despite achieving CIA, non-repudiation, and secrecy to a certain extent, the authors did not manage to accomplish optimal performance in the terms of latency.

**Threats:** T1.1.1 - Information leakage/sharing due to human errors, T1.3.1 - Device modification, T1.3.3 - Lack of control on safety implications - COVID-19, T1.4.2 - Denial of service, T1.4.3 - Malicious code/software/activity, T1.5.1 - Violation of laws or regulations, T1.4.5 - Failures of business process, T1.6.1 - Skill shortage, T1.6.2 - Lack of strong cyber hygiene practices – COVID-19

**Gaps:** G1.1 - Gaps in design, G1.2 - Gaps on protection mechanisms adoption and hardening, G1.5 - Lack of awareness and knowledge (skill shortage), G1.6 - Lack of interoperability, G1.8 - Fragmentation in security approaches and regulations, G1.10 - Gaps in cyber hygiene practices

**RA1.3 – Novel authentication schemes.** As suggested by El-hajj et al. [33], IoT authentication factors can be classified based on the following factors: i) authentication factor (based on the identity and the context of usage), ii) use of tokens (token-based and non-token based authentication schemes), iii) authentication procedure (one-way, two-way, and three-way authentication schemes), iv) authentication architecture (distributed and centralized authentication schemes), v) IoT layer (perception, network, and application layer authentication schemes), vi) hardware (implicit hardware-based and explicit hardware-based authentication schemes). When it comes to smart grids, the current trend seems to be leaning toward schemes based on Hash-based Message Authentication Code (HMAC), as it can be perceived from the several research efforts [34] [35] [36] [37], whereas novel schemes based on Physical Unclonable Function (PUF) are prevalent in smart RFID [38] [39] [40], smart homes [41] [42] [43] and generic IoT applications [44] [45] [46]. Future research endeavours in those fields should focus to combine both hardware and software solutions to further bolster security. Moreover, IoT applications for smart grids and VANETs location, and privacy should be considered. Research on wireless sensor networks recently focused on accomplishing mutual authentication [47] [48] [49] [50] through lightweight authentication schemes, such as Hash operations and ECC. The effectiveness of the existing protocols and schemes should be further analyzed against malicious activities and especially omnipresent DoS attacks. Moreover, future authentication schemes and protocols should be designed with low communication overhead and computation costs in mind, especially for resource-constrained IoT environments. At the same time, novel authentication schemes should be able to operate with the ever-growing number of nodes without having to be modified. Finally, as a general rule, authentication schemes should cater to all three IoT architecture layers, namely application, network, and perception layer.

**Threats:** T1.1.1 - Information leakage/sharing due to human errors, T1.1.2 - Inadequate design and planning or incorrect adaptation, T1.1.3 - Inadequate design and planning or incorrect adaptation in the critical scenario - COVID-19, T1.2.1 - Interception of information, T1.2.2 - Unauthorized acquisition of information (data breach), T1.4.1 -

Identity fraud, T1.4.2 - Denial of service, T1.4.4 - Misuse of assurance tools, T1.4.7 - Device hijacking, T1.4.8 - Social engineering

**Gaps:** G1.1 - Gaps in design, G1.2 - Gaps on protection mechanisms adoption and hardening, G1.3 - Gaps on authorization and authentication, G1.7 - Lack of security-dedicated budget, G1.12 – Gaps in insufficient data protection (communication and storage)

### Highlights on Identified Research Actions

There are three main areas in which future IoT cybersecurity research actions should be focused, namely ML/DL-based solutions, blockchain-based solutions, and development of the novel authentication schemes. ML and DL have the potential of mitigating privacy and access control issues and boosting capabilities of attack detection, intrusion detection, malicious code identification, and malware analysis in the IoT environments. Even though algorithms such as SVM, PCA, RNN, and ANN have already shown a certain degree of success in intrusion detection and identifying malicious activities, this area of research still requires significant effort to reach its full potential. Furthermore, more research on solving issues related to choosing appropriate training data, as well as parameter tuning, performance overhead, anomalies, and data validation and certification has to be conducted. The main properties of blockchain, including immutability, verifiability, and efficiency can aid in thwarting a large number of attacks targeting IoT systems. Besides that, blockchain solutions can help vendors to define configuration standards and access control for IoT. Future research endeavours must focus on further improving existing solutions in terms of performance, latency, and energy consumption. When it comes to the authentication schemes, current research trends lean towards lightweight authentication schemes, such as HMAC, PUF, ECC, and hash-based schemes. Future research should continue its focus on designing authentication schemes and protocols with low communication overhead and low computational costs that can operate with the growing number of nodes without having to be modified.

#### 3.2.2. Network-Centric Security

Based on the discussion of respective countermeasures identified regarding Network-Centric Security, these are briefly evaluated and complemented with a description of research actions foreseen.

##### 3.2.2.1. Countermeasures

We provide an overview of existing countermeasures that focus on one or more threats, and address gaps and challenges in Appendix A.2. This section aims to present the status of cybersecurity solutions connecting them to identified threats and gaps. We discuss classes of countermeasures, each describing the most relevant solutions to date.

**C2.1 -Vendor Process Evaluation and Product Assurance.** In addition to the secure standardized system and protocols, it is needed to have the assurance that also implementations are secure. Operators should implement effective supply-chain and procurement controls to ensure the services they operate and provide comply with security requirements and manage supply-chain threats. Industry-standard assessment programs to assure vendor products in support of the purchasing decision.

**Threats:** T2.4.1 - Failures of devices or systems, T2.4.2 - Supply chain, T2.4.3 - Software bug

**Gaps:** G2.1 - Gaps on security testing, on security accreditation schemes of network devices, and the massive deployment of PSIRT program from vendors. G2.16 - security of the new Open Radio Access Network model

**C2.2–Automated Patch Management.** The adoption of automated patch management allows proactively approaching the patching process by identifying systems that are non-compliant, vulnerable, or unpatched. Using software to automate and manage the patching process can allow for faster and more efficient patch management, simplifying the process of keeping operating systems and applications up to date. The implementation of automatic scanning permits to determine, which patches each system, software, or app is missing and then to send the appropriate patches to all relevant devices. Vendors should build, as much as possible, systems that permit their upgrade in a “hot” manner, reducing to the minimum the need to stop the services running on them.

**Threats:** T2.1.1 - Erroneous use or administration of devices and systems, T2.3.6 - Exploitation of vulnerabilities in services and remote tools - COVID-19, T2.3.4 - Remote activities (execution), T2.4.3 - Software bug

**Gaps:** G2.2 - Gaps on continuous hardening & patching of IT systems

**C2.3 - Security by default.** The supplier should provide network assets and functions that are securely configured by default according to state-of-the-art security configuration practices and should apply system hardening best practices. This includes restricting protocol access, removing or disabling unnecessary software, network ports, and services, removing unnecessary files, user accounts, restricting file permissions. In addition, implementing automatic network asset scanning can help in detecting deviations in system settings, and identify non-compliant devices.

**Threats:** T2.1.1 - Erroneous use or administration of devices and systems, T2.3.4 -Remote activities (execution), T2.3.6 - Exploitation of vulnerabilities in services and remote tools - COVID-19

**Gaps:** G2.2 - Gaps on continuous hardening & patching of IT systems

**C2.4 - Adoption of defensive solutions based on AI and ML.** Machine learning (ML) and AI applied to threat detection can help identify and prevent attacks. Threat actor payloads and attacks, including TTPs, are dynamic and ever-changing. A robust intelligence approach, requests to process big data, indicators of compromise coupled with context information, reputational data, and additional context. Leveraging ML and AI are essential to the timely and efficient processing of data, enhancing threat detection.

One possible use case involves the development of an ML/AI solution to detect a spam wave campaign underway in the wild. Common TTPs for this involve abuse of the email vector, unique cryptographic checksum hash value malware variants, and some common infrastructure if remote command and control infrastructure is used. It’s also common to target specific sectors. The manual, slow and inconsistent method relies on threat analysts examining individual tickets to attempt to quickly identify a potential threat and then informing a client or internal team of the threat. ML/AI can be used to process vast amounts of data across multiple clients and tickets in real-time, correlating those, providing granular attribution, coupled with orchestration and automation actions like auto-notify, and auto-defend actions (e.g. take an infected endpoint offline). In this context artificial intelligence or machine learning techniques can help to complement the security awareness training program in assisting to identify possible spam and phishing email, thus preventing the installation of malware that can be downloaded from malicious URL’s included in the body of email, artificially created to fool employers, or sent as attachments.

Another possible application of machine learning is to detect and mitigate malware. Microsoft was able to successfully implement ML (built into Windows Defense AV) to detect and mitigate Emotet malware<sup>43</sup>.

**Threats:** T2.1.1 - Erroneous use or administration of devices and systems

**Gaps:** G2.10 - Gaps on malware detection solution, G2.3 - Gaps on security training and awareness toward employees

**C2.5 – Periodic network security assessment.** For an understanding of the actual state of infrastructure, security assessment needs to be performed regularly, especially after reconfiguration or the addition of network equipment. By conducting regular external and internal penetration tests it is possible to identify vulnerabilities and attack vectors that can be used to exploit network systems successfully and to evaluate the effectiveness of the security measures in place. Testing should also cover the interfaces between the network nodes part of the infrastructures, between operators and providers, and customers.

**Threats:** T2.2.1 - Signaling traffic interception, T2.2.2 - Data session hijacking, T2.4.3 - Software bug, T2.3.7 - Exploitation of System Administrative Tools, T2.3.4 - Exploitation of application programming interfaces (APIs)

**Gaps:** G2.4 - Gaps on the massive deployment of mobile signalling firewalling solutions and anomaly detection systems specific to mobile signalling protocols, G2.6 – Gaps on best practice to increment GTP security assessment procedure and on a robust solution against Data session hijacking, G2.15 - Gaps on attack surface awareness, G2.17 - Gaps in the design of standards

**C2.6 – Monitoring & Event Analysis.** Network operators sometimes ignore that their networks are exposed to external threats. By monitoring network traffic at the interconnection points they can determine the effectiveness of existing configurations, of the measures in place, and highlight vulnerabilities and risks. This is especially important each time that network equipment is added or reconfigured. Only by constantly monitoring the traffic coming into the network, it is possible to detect events like BGP hijacking and to detect the BGP routes taken by network traffic and abnormal route change. Similar measures apply in the context of mobile networks. GTP Inspection and GTP Firewall are useful tools for monitoring GTP traffic and detecting potential security threats that come from the Internet. The *FS.11: SS7 interconnect security monitoring guidelines document* from GSMA, describes how to monitor SS7 traffic for potential attacks and how to classify incoming signalling messages that arrive on the interconnection interface.

**Threats:** T2.2.1 Signaling traffic interception, T2.2.2 - Data session hijacking, T2.3.7 - Exploitation of System Administrative Tools, T2.3.4 - Exploitation of application programming interfaces (APIs)

**Gaps:** G2.4 - Gaps on the massive deployment of mobile signalling firewalling solutions and anomaly detection systems specific to mobile signalling protocols, G2.6 – Gaps on best practice to increment GTP security assessment procedure and on a robust solution against Data session hijacking, G2.14 - Gaps on Defense in Depth, G2.15 - Gaps on attack surface awareness, G2.17 - Gaps in the design of standards

**C2.7 – Adoption of End-to-end security approach.** Interconnect protocols have been designed without security in mind. Several solutions have been proposed to secure SS7 and Diameter but have never been adopted by the industry (MAPsec, TCAPsec, Diameter over IPsec, Diameter over SCTP/DTLS). A good approach is to implement end-to-end security solutions, providing both confidentiality and integrity to sensitive exchanges. In this case, the choice for the network operators is to establish secure bi-directional links with a small

---

<sup>43</sup> <https://www.microsoft.com/security/blog/2018/02/14/how-artificial-intelligence-stopped-an-emotet-outbreak/>

number of partners providing source authentication, integrity, and confidentiality. However, such a solution would never apply to all roaming partners. The common practice to implement interconnection is via an IPX carrier. In this scenario, operators must request to IPX carriers the adoption of security requirements.

**Threats:** T2.2.1 - Signalling traffic interception.

**Gaps:** G2.4 - Gaps on the massive deployment of mobile signalling firewalling solutions and anomaly detection systems specific to mobile signalling protocols

**C2.8 – Adoption of Formal verification methods in the security protocol design process.** Protocols must be tested for their functional correctness before they are used in practice. Application of formal methods for verification of security protocols would enhance their reliability thereby, increasing the usability of systems that employ them. Formal security verification methods and schemas should be adopted by the specification and standardization bodies, to identify and address possible security issues since the initial steps of their definition. This will result in more robust specifications of networks, reducing time and efforts in addressing security issues when the products are already in place, limiting the impact of design security weaknesses.

**Threats:** T2.3.1 - Exploitation of software bugs, T2.3.4 - Exploitation of application programming interfaces (APIs)

**Gaps:** G2.5 – Gaps in the standardization process to include formal security verification and security assessment/testing of new protocol/network specifications, G2.17 - Gaps in the design of standards

**C2.9 - Protection at the network or transport layer with mutual authentication.**

Secure protocol on network or transport layer, providing confidentiality, integrity, and replay protection like IPSEC and DTLS, should be adopted for both user and control plane, particularly in the untrusted portion of the network such as access network or roaming interconnection. Mutual authentication between network functions should be enabled for transport protection by using protocols like TLS with X.509v3 certificates to prevent access from a fake network component. Authorization to access resources provided by network function should be also enforced by enabling authorization mechanisms like OAuth 2.0. Protection of DNS traffic using digital signatures based on public-key cryptography (DNSSEC).

**Threats:** T2.2.3 - Traffic Eavesdropping, T2.2.4 - Traffic redirection, T2.3.4 - Exploitation of application programming interfaces (APIs)

**Gaps:** G2.7 – Gaps on the deployment of the robust crypto algorithm to cipher user plane traffic while minimizing performance impact and interoperability issues. G2.8 – Gaps on robust and innovative solutions to protect DNS traffic systems, G2.17 - Gaps in the design of standards

**C2.10 – Adoption of strong and secure protocols.** Strong, ciphering and integrity protection algorithms should be enabled by default, to protect data from interception and modification, of both user and signalling data exchanged, between the user equipment and the network. Deprecated algorithms (such as TLS 1.1), but also obsolete protocol versions kept working only for legacy reasons (e.g. TLS 1.2) should not be enabled, using instead industry-standard network protocols with sufficient security measures and industry-accepted algorithms.

**Threats:** T2.2.3 - Traffic Eavesdropping

**Gaps:** G2.7 – Gaps on the deployment of the robust crypto algorithm to cipher user plane traffic while minimizing performance impact and interoperability issues

**C2.11 - Threat Intelligence Integration and Automation.** To increase SOC productivity and accelerate incident investigations SOAR (advanced orchestration, automation, and response capabilities) technologies should be adopted. These are based on three distinct technologies: security orchestration and automation, security incident response platforms

(SIRP), and Threat Intelligence Platforms (TIP). By adopting SOAR, the SOC can rely on the standardized process for data aggregation that assists human and machine-led analysis and automates detection and response processes, allowing analysts to focus on the tasks that require deeper human analysis and intervention.

**Threats:** T2.3.3 - Malicious code/software/activity, T2.3.6 - Exploitation of vulnerabilities in services and remote tools - COVID-19

**Gaps:** G2.13 - Gaps on the reduced capacity to perform security operations

**C2.12 - Adoption of cooperative DDoS attack detection and mitigation.** A countermeasure to fight DDoS attacks is to adopt a cooperative approach across organizations and sectors through the sharing of expertise and experiences, the sharing of measurements of the properties of DDoS attacks and information about DDoS attacks. In this direction is the initiative carried out inside CONCORDIA related to the T3.2 (Piloting a DDoS Clearing House for Europe) and T3.1 (Building a Threat Intelligence for Europe)

**Threats:** T2.3.5 - Malicious code - Signalling amplification attacks

**Gaps:** G2.11 - Gaps on containing amplification attacks

**C2.13 - Adoption of enhanced filtering, cross-correlation mechanisms.** The complexity of network deployments, related to the need to interwork with other network functions, to interoperate with the legacy network, to support different use cases and security configurations, opens to potential attack paths that exploit the lack of cross-validation between different layers. A pure IP layer firewall or general transport layer security solution cannot provide such a holistic approach, as it does not have the understanding of the interaction of the layers, such as, whether the slice identity in the actual signalling layer request matches the transport layer, or if a UE identity belongs to a slice or not. Therefore, the deployment of an IP firewall gives a false sense of security, as the controls provided by it can be bypassed on the signalling layer. Adoption of enhanced filtering and validation approach, which combines information from different layers, protocols and integrates external threat information is a necessary countermeasure to detect complex attacks. Cross-correlation of attack information maximizes the protection against sophisticated attackers and allows better mitigations and faster detection while minimizing false sense of security.

**Threats:** T2.2.1 - Signalling traffic interception, T2.3.8 - Attacks to sliced 5G core network

**Gaps:** G2.5 – Gaps in the standardization process to include formal security verification and security assessment/testing of new protocol/network specifications, G2.17 - Gaps in the security of network slicing

**C2.14 - Managing firmware updates and hardware.** Management of firmware includes several aspects such as updating firmware, secure setting of firmware, and monitoring of firmware. Network devices should be configured to check for the existence of firmware updates at frequent intervals. Automatic firmware updates should be enabled by default assuring that the update server is secure, that the update file is transmitted via a secure connection, that it does not contain sensitive data (e.g. hardcoded credentials), that it is signed by an authorized trust entity, and encrypted using accepted encryption methods, and that the update package has its digital signature, signing certificate, and signing certificate chain, verified by the device before the update process begins.

**Threats:** T2.3.2 - Manipulation of hardware and firmware

**Gaps:** G2.9 – Gaps on wide adoption of integrity-protected firmware also in IoT system

### Highlights on Identified Countermeasures

The security assurance of network components certifying that a particular product has been designed and developed with a specified level of security, according to the given standards is a requisite for deploying secure network architectures. This means that supply chain risk assessment and product testing shall be in place, ensuring that vendors offer appropriate

security protection and are accountable for security lapses, especially in heterogeneous networks where there may be an increase in the number of vendors.

Network deployment shall follow security best practices and guidelines in terms of activation of security features, hardening of the configuration, network segmentation and protection of internal interfaces from external access. Network monitoring solutions provide visibility of network security, giving greater insight into the traffic entering the network and its behaviour. Where applicable, usage of automation and machine learning shall be integrated into network operation and management processes. Internal vulnerability management procedures have to be reviewed and adapted to be more effective with an aggressive timeline in patching and staying aligned with security updates. Although measures should be taken to mitigate the risk of 0-day vulnerabilities, patching publicly known vulnerabilities as quickly as possible significantly reduces the risk of exploitation.

### 3.2.2.2. Research Actions

We provide a discussion on relevant research actions that need to be taken to mitigate the threats, gaps, and challenges previously identified and reported in Appendix A.2.

**RA2.1 - Machine Learning.** Over the past decade, the role of machine learning in cybersecurity has grown, as the threats become more serious and as the technology becomes more advanced. Machine learning methods have been effectively used in the prevention and detection stage of network threats. The analysis of the main network threats, highlights that one of the main needs in the prevention stage, is the availability of tools that can autonomously find and patch vulnerabilities to eliminate potential network weaknesses. Penetration testing is commonly used to look for publicly known vulnerabilities and insecure configurations in the network by planning and generating possible attack exploits. However, network penetration testing requires a significant amount of training and time to perform well. Some automated tools, like Metasploit,<sup>44</sup> can partially reduce these costs, but these tools simply run through a list of pre-selected, known exploits to determine if any machines on a network are vulnerable to them. Recently machine learning has emerged as a plausible way of doing penetration tests [51]. Current approaches to automated penetration testing have relied on methods that require a model of the exploit outcomes; however, the cyber security landscape is rapidly changing as new software and attack vectors are developed which makes producing and maintaining up-to-date models a challenge. To try and address the need for the exploit, the application of machine learning technique, namely Reinforcement Learning (RL), has been investigated. RL is an AI optimization that does not require a model of the environment to produce an attack tactic and instead learns the best tactic through interaction with the environment.

Schwartz et al. [52] have proven that the RL algorithm can automatically exploit vulnerabilities on networks and deploy attacks on target machines. On the other hand, Ghanem et al. [53] suggested the capacity to integrate RL with existing PT systems to execute tasks without human intervention. However, studies exploring the use of reinforcement learning for penetration testing typically rely on small environments, often simulated networks of around ten machines with a limited number of exploits provided to the program. As either the complexity of the environment or the number of actions available to the program increases, reinforcement learning can quickly become computationally prohibitive. New research in the context of penetration testing, based on reinforcement

---

<sup>44</sup> metasploit-framework, <https://github.com/rapid7/metasploit-framework>  
www.concordia-h2020.eu

learning, should be focused on developing computationally feasible methods of simulating complex networks that can scale to the size of modern large networks, while also handling hundreds of possible exploits. As the next step, these algorithms should be applied in more realistic environments such as VM networks using information from real organizational networks to determine how they can be applied in real-world settings.

Beyond finding vulnerabilities with autonomous penetration testers, another topic that may need future research is related to the use of machine learning in vulnerability assessment and management prioritization. In their work of Jacobs et al. [54] have used data about attacks observed in the wild to build machine learning systems that predict the likelihood of some vulnerabilities being exploited. Jacobs et al. [55] evaluated the use of machine learning-based risk assessments in conjunction with the CVSS (Common Vulnerability Scoring System) to prioritize the vulnerabilities that are most likely to be exploited. Fang et al. [56] proposed a model to predict the exploitability and exploitation in the wild of vulnerabilities by grasping the key features of the vulnerability. Further research is needed to improve the accuracy and quality of exploits labelling, exploit database, and the proof of exploits in the wild. More data sources with high coverage and time efficiency should also be investigated.

In the detection phase, several researchers have focused on the use of ML for network intrusion and malware detection systems. Intrusion detection systems are typically classified as either misuse-based or anomaly-based. Both methods can make use of different ML methods. The simplest forms of misuse-based detection rely on known indicators of compromise. It allows identifying malicious events quickly and accurately, thanks to the high processing speeds and low false-positive rates. However, since it is based on known threats it doesn't protect against novel attacks. ML can be used to automate some forms of misuse-based detection by allowing a system to "learn" what different types of attacks look like. If many examples of past attacks are available, a supervised learning classifier can be trained to identify the signs of different types of attacks, without the need for humans to generate specific lists of rules that would trigger an alert. Different from misuse-based detection, anomaly-based detection flags suspicious behavior without making specific comparisons to past attacks allowing for potential identification of novel attacks.

This type of detection system is more likely to use unsupervised learning methods to cluster normal traffic within a network and alert as suspicious any activity which deviates from that pattern. However, this type of detection is prone to generate many false positives that are expensive to investigate. This is mainly since normal traffic can be highly variable; just as an example, last year in response to COVID-19 millions of employees suddenly began working from home. This has profoundly changed the "usual/normal" network's traffic profile. Research in this area has focused on finding ways to appropriately baseline "normal" traffic for a given network. Moreover, the massive increase in network traffic and the resulting security threats have posed many challenges to detect malicious intrusions efficiently. A research challenge of machine learning is the unavailability of a systematic dataset that reflects the new network attacks. Most of the proposed methodologies are not able to detect zero-day attacks because these models are not trained with enough attack types and patterns. New research should test and verify ML models using the dataset having older and newer attacks. On the other hand, dataset construction is an expensive process that demands a lot of resources and high knowledge. Hence, one of the research challenges is the systematic construction of an up-to-date dataset with enough instances of almost all the attack types. The dataset should be updated frequently to include the latest intrusion instances.

Another challenge is related to the lower detection accuracy for certain attack types against the overall detection accuracy of the ML model used. This problem is caused by the

imbalanced nature of the dataset so that detection accuracy for the low frequent attacks class is lower than the attacks with more instances. Research in this context requires coming up with an up-to-date and balanced dataset and with efficient techniques that can increase the number of minority attack instances to balance the dataset. Recently, certain techniques like SMOTE [57], RandomOverSampler, and adaptive synthetic sampling approach (ADASYN Algorithm), have been proposed for reducing the dataset imbalance ratio for improved performance. But there is still room for improvement and more research in this direction is needed.

Several Deep Learning-based algorithms have also been studied for application in network intrusion detection showing effective results in detecting malicious attacks due to deep feature learning ability. DL is the subset of the ML which includes many hidden layers to get the characteristics of the deep network. These techniques are more efficient than the ML due to their deep structure and ability to learn the important features from the dataset on its own and generate an output. However, they are quite complex and require high resources in terms of computational power, storage capacity, and time, and therefore rising some challenges to be implemented in real-time environments. Future direction should also explore the hybrid idea of using DL for feature extraction and ML for classification to reduce the complexity. Other studies [57] have also evaluated the use of a Deep Learning Approach for IP Hijack Detection.

Future research should also investigate the use of machine learning in the context of active defence in the intent to try to study potential adversaries to better anticipate their actions. This is related to the Threat Intelligence activity in terms of means to gather threat intelligence about potential adversaries through the analysis of collected data. Some researchers have explored how ML and text mining can be used to improve threat intelligence analysis. For instance, ML methods can be used to cluster dark web users, or text mining methods could be leveraged to automatically collect, classify, and analyze posts on dark web forums and marketplaces, allowing researchers to identify zero-day exploits before they are deployed [58]<sup>45</sup>. In this context, a fully automated ML system could help in anticipating vectors of attack by searching potential vulnerabilities mentioned on the dark web impacting an organization's name or a list of its products.

Other tools introduced as deceptive tactics could be repurposed to collect threat intelligence about potential adversaries. For example, information related to an attack including the tactics used, the country of attack, and so on can be clustered and used by ML methods to identify similar attacks [59] [60]<sup>46</sup>.

**Threats:** T2.1.1 - Erroneous use or administration of devices and systems, T2.2.2 - Data session hijacking, T2.3.1 - Exploitation of software bugs, T2.3.3 - Malicious code/software/activity, T2.3.4 - Remote activities (execution), T2.3.6 - Exploitation of vulnerabilities in services and remote tools - COVID-1, T2.3.8 - Attacks to sliced 5G core network, T2.3.5 - Malicious code - Signalling amplification attacks; T2.4.3 - Software bug

**Gaps:** G2.2 - Gaps on continuous hardening & patching of IT systems, G2.3 – Gaps on security training and awareness toward employees, G2.10 - Gaps on malware detection solution, G2.13 - Gaps on the reduced capacity to perform security operations, G2.15 - Gaps on attack surface awareness, G2.16 – Gaps on the security of the new Open Radio Access Network model

**RA2.2 –Quantum-safe cryptography and security.** The advent of large-scale quantum computing brings a significant threat to information infrastructure. Popular cryptographic

<sup>45</sup>Artificial intelligence shines light on the dark web, <https://news.mit.edu/2019/lincoln-laboratory-artificial-intelligence-helping-investigators-fight-dark-web-crime-0513>

<sup>46</sup>Machine Learning Support for Cyber Threat Attribution at FireEye, <https://www.fireeye.com/blog/products-and-services/2020/06/machine-learning-support-for-cyber-threat-attribution-at-fireeye.html>

schemes, like RSA and Elliptic Curve Cryptography, based upon mathematical problems that are believed to be difficult to solve, given the computational power available now, will be easily broken by a quantum computer. This will rapidly accelerate the obsolescence of currently deployed security systems and will put at risk of eavesdropping on information transmitted on public channels. Even encrypted data that is safe against current adversaries can be stored for later decryption once a practical quantum computer becomes available. At the same time, it will be no longer possible to guarantee the integrity and authenticity of transmitted information, as tampered data will go undetected. Hence, communications will become insecure without additional action such as using quantum-safe cryptography and exploiting enablers such as Quantum Key Distribution.

Quantum-safe cryptography refers to efforts to identify algorithms that are resistant to attacks by both classical and quantum computers. Post Quantum Cryptography (PQC) represents today one of the most interesting topics for cryptographic research. Post-quantum cryptography has to maintain integrity and confidentiality while preventing different kinds of attacks. Research is typically concentrated on six techniques such as symmetric key quantum resistance, super-singular elliptic curve isogeny cryptography, code-based cryptography, hash-based cryptography, multivariate cryptography, and lattice-based cryptography [61].

NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms<sup>47</sup>. Some challenges however exist: the reconfiguration of legacy devices with cryptosystems is still an open problem, which needs to be solved. To adapt to post-quantum cryptography transition in real-time applications, there is a need to formalize a wide array of standards. For example, integration with mobile communications, emergency services, and critical infrastructure requires studying post-quantum algorithm choices. Just as an example, there is a critical need to ensure that 5G and future standards, will be developed, envisioning future adoption of PQC for public-key ciphers.

**Threats:** T2.2.3 - Traffic eavesdropping, T2.2.4 - Traffic redirection

**Gaps:** G2.5 – Gaps in the standardization process to include formal security verification and security assessment/testing of new protocol/network specifications, G2.7 – Gaps on the deployment of the robust crypto algorithm to cipher user plane traffic while minimizing performance impact and interoperability issues.

### Highlights on Identified Research Actions

Future research actions on network cybersecurity should be focused on AI, and on ML-based solutions, and start to foresee the use and integration of Quantum-Safe Cryptography. Artificial Intelligence (AI) and Machine Learning (ML) have the potential for use in a wide range of network activities including service orchestration, demand management, security response and analytics. AI and ML are playing an increasingly important role in cybersecurity, powering security tools that can analyse data from millions of previous cyber incidents and use it to identify in the fastest timeframe, potential threats or new variants of malware allowing quick mitigation reactions.

These tools are particularly useful if we consider that cybercriminals are always trying to modify their malware code so that security software is no longer able to recognise it as malicious. But detecting new kinds of malware isn't the only way that AI and ML technologies can be deployed to enhance cybersecurity: an AI-based network-monitoring

---

<sup>47</sup> Post-Quantum Cryptography PQC, <https://csrc.nist.gov/projects/post-quantum-cryptography>

tool can also track what users do on a daily basis, building up a picture of their typical behavior. By analysing this information, the AI can detect anomalies and react accordingly. This way AI and ML enable cybersecurity teams to respond in an intelligent way, understanding the relevance and consequences of a breach or a change of behaviour, and developing in real-time an adequate response. The more cybersecurity will become reliant on AI and ML, the more AI and ML will be a target of malicious attacks. Moreover, also hackers will use AI to improve their malware to make it resistant to AI-based security tools. Improvements in Quantum computing may allow to break some cryptographic protocols in a more practical way. This means that communications will become insecure without additional action such as using quantum-safe cryptography and exploiting enablers such as Quantum Key Distribution.

There is much activity already underway and the latest requirements for cryptographic protocols for mobile telecommunications have been defined with the need to be quantum-safe in mind. In this context one of the main topics is related to Quantum-secure communications, AKA quantum key distribution (QKD), that is at the heart of every secure communication (essential for both: fibre-based communication, but also for satellite communications), although the most controversial application of Quantum Computing is related to the breaking of current public-key cryptography.

An emerging research topic is Quantum machine learning, which is the integration of quantum algorithms within machine learning programs. While machine learning algorithms are used to compute immense quantities of data, quantum machine learning utilizes qubits and quantum operations or specialized quantum systems to improve computational speed and data storage done by algorithms in a program. Hence Quantum computing can help to improve classical machine learning algorithms and its applications to cybersecurity. Ideas range from running computationally costly algorithms or their subroutines efficiently on a quantum computer to the translation of stochastic methods into the language of quantum theory.<sup>48</sup>

### 3.2.3. System-Centric Security

Based on the discussion of respective countermeasures identified regarding System-Centric Security, these are briefly evaluated and complemented with a description of research actions foreseen.

#### 3.2.3.1. Countermeasures

We provide an overview of existing countermeasures that focus on one or more threats, and address gaps and challenges in Appendix A.3. This section aims to present the status of cybersecurity solutions connecting them to identified threats and gaps. We discuss classes of countermeasures, each describing the most relevant solutions to date.

**C3.1 - Firewalls.** Firewalls running in a virtualized environment can provide functionalities for packet filtering and services monitoring and can execute in hypervisor and bridge modes [62]. Hypervisor firewalls protect VMs by monitoring VM activities and sifting malicious from good traffic. To enable these firewalls, the physical host hypervisor kernel has to be modified to allow the firewalls to access VM information and virtualized network interfaces

---

<sup>48</sup> An introduction to quantum machine learning, M. Schuld, I. Sinayskiy, F. Petruccione, Contemporary Physics doi:10.1080/00107514.2014.964942

[63]. That way hypervisor firewall can run without being in contact with the virtual network. Furthermore, perimeter and internal firewalls should be used for controlling both private and public network traffic within and outside the cloud systems, as well as detecting possible anomalies. Lastly, firewalls should be used for separating groups of VMs from production and development hosted groups<sup>22</sup>.

**Threats:** T3.4.3 - Malicious code/software/activity, T3.4.7 - Code execution and injection (unsecured APIs), T3.4.8 - Generation and use of rogue certificates, T3.4.9 – State-sponsored attacks

**Gaps:** G3.12 - Gaps on insider threat, G3.18 - Gaps on malware exposure, G3.23 - Gaps on remote network controls

**C3.2 - Encryption and key management.** Cryptography is one of the most essential means of mitigating security issues in virtualized environments. Organizations should define policies of the use of encryption and controls of cryptographic authentication and integrity, including digital signatures and key management<sup>49</sup>. There are three distinct phases for protecting data in virtual environments, namely encryption of data-at-rest (protecting data from illegal acquisition and malicious CSP), encryption of data-at-transit (encrypting confidential information during internet transmission), and encryption of data on backup media (protection of misuse of stolen data) [63]. VPN should be used to secure communication between distributed systems since they feature cryptographic tunnelling protocols which enable confidentiality and authentication<sup>22</sup>.

**Threats:** T3.2.1 - Interception of information, T3.2.2 - Unauthorized acquisition of information (data breach), T3.4.1 - Identity fraud

**Gaps:** G3.1 - Gaps on the use of cryptography, G3.2 - Gaps on data control, G3.11 - Gaps on insufficient identity, credential, access, and key management

**C3.3 - Virtual Trusted Platform Module (vTPM) and Trusted Virtual Domains (TVDs).** Virtual Trusted Platform Module (vTPM) is linked to physical trusted platform modules (TPMs) through a certificate chain and is located in a specific hypervisor layer. An instance of vTPM that emulates TPM functionality for extending the chain of trust to vTPM is created for each distinct VM, where it can be invoked by a hypervisor. In the case of multitenant virtualized cloud environments, physical TPM is virtualized so it can be used by multiple VMs on a single platform. Trusted virtual domains (TVDs) are formed by clustering the related VMs on the physical machine into a platform that uses a unified security policy defined by the administrator. Malicious VMs are blocked from joining TVDs and affecting VMs of trusted users through policy requirements. Each VM on TVD has a unique identifier, which serves for identifying the assigned VMs to specific end-users and enabling VMs to run on TVD which follows predefined security guidelines and policies [63] [64].

**Threats:** T3.2.1 - Interception of information, T3.2.2 - Unauthorized acquisition of information (data breach), T3.4.3 - Malicious code/software/activity, T3.4.4 - Generation and use of rogue certificates, T3.6.2 - Malicious insider

**Gaps:** G3.1 - Gaps on the use of cryptography, G3.2 - Gaps on data control, G3.3 - Gaps on multi-tenancy, isolation, and resource management

**C3.4 - Enforcing Access Control Mechanisms (ACMs).** Access control management (ACM) mechanisms for users, applications, and systems are essential for mitigating the issue of authorization abuse, as well as granting the integrity and

---

<sup>49</sup>ISO 27001 suggests the use of cryptography to deal with unintentional leakages and prevent unauthorized access to sensitive data and systems. However, encryption key management is challenging. Also according to NIST publications, the security for cryptographic keys adds an additional complexity, due to more consumer-provider relationships and the variety of infrastructures “on which both the key management system and protected resources are located”.

confidentiality of resources. In virtual cloud environments, ACMs operate according to predefined security policies by restricting or limiting access to systems or processes. In VM image libraries, along with strong ACMs, each image should also use a digital signature<sup>50</sup>. For the hybrid cloud, organizations should implement granular access control and utilize two distinct authentication zones (for internal and external systems) to mitigate the risks caused by compatibility issues of using both private and public clouds at the same time.<sup>51</sup> Some of the most popular ACM solutions include Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-Based Access Control (RBAC) [65], and more recently Chipertext-Policy Attribute-Based Encryption (CP-ABE) [66].

**Threats:** T3.2.1 - Interception of information, T3.2.2 - Unauthorized acquisition of information (data breach), T3.4.1 - Identity fraud, T3.4.9 – State-sponsored attacks, T3.6.2 - Malicious insider

**Gaps:** G3.1 - Gaps on the use of cryptography, G3.2 - Gaps on data control, G3.16 - Gaps on account hijacking due to the inadequate authentication

**C3.5 - Maintaining proper configuration of virtualized and cloud environments.** Each component in a virtualized environment has a specific configuration. Due to the ease of cloning and copying VMs' images, mitigation of all potential configuration risks is crucial<sup>52</sup>. Hence, the configurations should be periodically assessed to maintain the trusted state of the virtual environment. Every configuration change should be documented adequately. Moreover, there are specialized tools, including CloudSploit and Dome9 that can be used for identifying configuration security issues<sup>22</sup>. To ensure environmental stability and thwart potential threats, proper configuration audit and control should be established according to the defined standards. ISACA<sup>53</sup> recommends regular policy and control evaluations, synchronization, services, and file sharing configuration check-ups. Furthermore, a configuration management database (CMDB) should be maintained and information regarding suspended VMs' images and physical-to-virtual mapping should be properly recorded.

**Threats:** T3.3.1 - Configuration poisoning, T3.4.2 - Denial of service, T3.4.9 – State-sponsored attacks

**Gaps:** G3.9 - Gaps on misconfiguration and inadequate change of control, G3.12 - Gaps on insider threat, G3.23 - Gaps on remote network controls, G3.24 – Gaps on the configuration of cloud storage

**C3.6 - Isolating guest operating systems.** Since guest OSs and their corresponding virtual machines are the main building blocks of the virtualized environment, they have to be isolated and partitioned to mitigate potential propagation and infection of the malicious control boundaries. On top of that, virtual machines of guest OSs should be properly hardened, and security controls should be layered. Guest OSs should be updated promptly, and each guest OS should use different authorization credentials. In the case that one guest OS is compromised, all remaining guest OSs using the same hardware have to be assumed to be compromised. Guest OSs should also be examined regularly for a potential compromise.

**Threats:** T3.3.2 - Business process poisoning, T3.4.9 – State-sponsored attacks

**Gaps:** G3.3 - Gaps on multi-tenancy, isolation, and resource management, G3.19 - Gaps on race conditions

**C3.7 - Monitoring and maintaining hypervisor/VMM activities.** A single point of failure in the hypervisor can affect the entire virtualized environment, thus it is of the essence to

---

<sup>50</sup> See <http://www.nist.gov>

<sup>51</sup> See <https://cloudsecurityalliance.org>

<sup>52</sup> Security aspects of virtualization, <https://www.enisa.europa.eu/publications/security-aspects-of-virtualization>

<sup>53</sup> See <http://www.isaca.org/>

properly secure it. The hypervisor should always be kept updated with the latest patch releases either automatically or through centralized patch management. Administrative access to the management interface of the hypervisor should be restricted and the virtualized infrastructure to a trusted authoritative time server should be kept synced. To maintain required security measurements, self-integrity and introspection monitoring capabilities can be used for monitoring the activities of guest OSs and hypervisor itself. Lastly, services that could open the door to possible attacks, such as clipboard and file-sharing services should be disabled, while unused hardware should be disconnected.

**Threats:** T3.4.2 - Denial of service, T3.4.3 - Malicious code/software/activity, T3.4.4 - Generation and use of rogue certificates, T3.4.7 - Code execution and injection (unsecured APIs), T3.4.9 – State-sponsored attacks, T3.6.2 - Malicious insider

**Gaps:** G3.6 - Gaps on forensics, G3.5 - Gaps on security assurance and Service Level Agreements (SLAs), G3.8 - Lack of visibility/control, G3.12 - Gaps on insider threat, G3.18 – Gaps on malware exposure, G3.20 – Gaps on logistic challenges to the ever-increasing cloud usage

**C3.8 - Making systems secure by default.** Every system should provide minimum security requirements through the deployment and configuration of a minimum set of security controls, which should be logged and audited. That way previous actions or sequences of actions can be traced back. Moreover, security dependencies and trust boundaries between different components are essential for virtual networks and should be thus clearly defined. New security protocols should strictly follow predefined definitions of security objectives, impact evaluation, and backward compatibility.

**Threats:** T3.1.2 - Inadequate design and planning or incorrect adaptation, T3.4.3 - Malicious code/software/activity, T3.4.5 - Misuse of assurance tools, T3.4.6 - Failures of the business process, T3.4.9 – State-sponsored attacks

**Gaps:** G3.14 - Gaps on abuse and nefarious use of cloud services, G3.15 - Gaps on insecure interfaces and APIs, G3.21 - Gaps on endpoint controls, G3.20 – Gaps on logistic challenges to the ever-increasing cloud usage

**C3.9 - Raising security awareness.** One of the most important security measures for ensuring the success and growth of cloud and virtualization platforms is raising security awareness among organizations and end-users. It involves educating end-users (employees) on the potential cybersecurity vulnerabilities and threats and instigating them with the best practices and procedures available. Besides preventing possible security breaches and related financial losses, an organization with security-aware employees can yield benefits related to the reputation, which could help to gain more customers and thus increase its profit. Therefore, security awareness campaigns and proper training are of utmost importance for both end-users and organizations.

**Threats:** T3.1.1 - Information leakage/sharing due to human errors, T3.1.2 - Inadequate design and planning or incorrect adaptation, T3.4.6 - Failures of the business process, T3.4.8 - Phishing - COVID-19, T3.4.9 – State-sponsored attacks, T3.6.1- Skill shortage, T3.6.3 - The lack of awareness - COVID-19, T3.6.4 -Personal cloud service adoption - COVID-19, T3.6.5 - Cloud sprawl - COVID-19

**Gaps:** G3.4 - Gaps on roles and human resources, G3.6 - Gaps on forensics, G3.10 - Gaps on lack of cloud security architecture and strategy, G3.22 - Gaps on Cloud user awareness

**C3.10- Enforcing regulations.** More regulations are necessary for ensuring that manufacturers and vendors prioritize security and provide guidelines on the use of the cloud, and thus providing the necessary level of transparency to the organizations and end-users. Programs and policies such as CSAs Security, Trust and Assurance Registry (STAR)

program<sup>54</sup> and the EU General Data Protection Regulation (GDPR)<sup>55</sup> should be enacted across the global level. STAR program, which is globally used by customers, providers, industries and governments provides different assurance requirements and maturity levels of providers and end-users, while the GDPR introduced mandatory notification schema which coerces data controllers to report data breaches promptly. In addition, GDPR guarantees that data controllers deal with data breaches in accordance to the predefined guidelines<sup>56</sup>.

**Threats:** T3.4.5 - Misuse of assurance tools, T3.5.1 - Violation of laws or regulations, T3.6.5 -Cloud sprawl - COVID-19

**Gaps:** G3.5 - Gaps on security assurance and Service Level Agreements (SLAs), G3.7 - Gaps on standards/regulations, G3.10 - Gaps on lack of cloud security architecture and strategy

### Highlights on Identified Countermeasures

Hypervisor firewalls can protect VMs by monitoring their activities and separating good from malicious traffic, while internal firewalls can control both public and private network traffic within and outside the cloud. Protecting data in a virtual environment is performed in three phases, namely encryption of data-at-rest, encryption of data-in-transit, and encryption of data on backup media. TVDs are formed by grouping the related VMs on the physical machine into a platform that uses unified security defined by the administrator while blocking compromised VMs. In the hybrid cloud, granular access control, as well as internal and external systems' authentications can be used for mitigating the compatibility issues of private and public clouds. To prevent cloning and copying of VMs' images and to sustain the trusted mode it is necessary to periodically access configurations. Both VMs and guest OSs have to be properly hardened and monitored regularly to mitigate the potential infection spreading. Moreover, self-integrity and introspection monitoring capabilities can be used to monitor and maintain required security actions of hypervisors and guest OSs. Lastly, every system should be designed in a way that provides minimum security requirements through the deployment and configuration of recorded security controls.

#### 3.2.3.2. Research Actions

We provide a discussion on relevant research actions that need to be taken to mitigate the threats, gaps, and challenges previously identified and reported in Appendix A.3.

**RA3.1 - SDN.** The advent of SDN that enables centralized control of network applications and devices, increased the efficiency of cloud services. It made possible for cloud services to deploy cross-storage spanning across many different locations around the globe, thus making storage management, way more efficient and less complex. Examples of cross-storage include multi-clouds, hybrid clouds, meta-clouds, and clouds federations<sup>57</sup>. World renown companies, such as Microsoft and IBM are working on the development of cross-

---

<sup>54</sup> Security Assurance in Cloud Adoption, [https://www.capgemini.com/wp-content/uploads/2017/07/security\\_assurance\\_in\\_cloud\\_adoption.pdf](https://www.capgemini.com/wp-content/uploads/2017/07/security_assurance_in_cloud_adoption.pdf)

<sup>55</sup> Chapin, M., *et al*; *Implication of the General Data Protection Regulation*, March 2018, [https://www.aacrao.org/docs/default-source/signature-initiative-docs/gdpr/gdpr\\_discussiondraft\\_03272018\\_v2.pdf?sfvrsn=4556dd66\\_0](https://www.aacrao.org/docs/default-source/signature-initiative-docs/gdpr/gdpr_discussiondraft_03272018_v2.pdf?sfvrsn=4556dd66_0)

<sup>56</sup> Bird & Bird, "Personal data Breaches and Notification," [https://www.twobirds.com/~/\\_media/pdfs/gdpr-pdfs/42--guide-to-the-gdpr--personal-data-breaches-and-notification.pdf?la=en](https://www.twobirds.com/~/_media/pdfs/gdpr-pdfs/42--guide-to-the-gdpr--personal-data-breaches-and-notification.pdf?la=en)

<sup>57</sup> SDN Security: Five reasons SDN is more secure than legacy networks, <https://codilime.com/five-reasons-sdn-is-more-secure-than-legacy-networks/>

storages, and particularly cross-cloud. Such solutions provide very high-security standards and enable administrators to manage the entire network from a single control panel. On top of that, this technology can aid in filtering out malicious traffic and in the case of an emergency, establish new virtual machines with minimal costs [67].

**Threats:** T3.1.2 - Inadequate design and planning or incorrect adaptation, T3.3.1 - Configuration poisoning, T3.4.3 - Malicious code/software/activity, T3.4.4 - Generation and use of rogue certificates, T3.4.6 - Failures of business process, T3.4.7 - Code execution and injection (unsecured APIs), T3.4.7 - Device hijacking, T3.5.1 - Violation of laws or regulations, T3.6.2 - Malicious insider, T3.6.5 - Cloud sprawl - COVID-19

**Gaps:** G3.2 - Gaps on data control, G3.3 - Gaps on multi-tenancy, isolation and resource management, G3.8 - Lack of visibility/control, G3.12 - Gaps on insider threat, G3.14 - Gaps on abuse and nefarious use of cloud services, G3.21 - Gaps on endpoint controls, G3.23 - Gaps on remote network controls

**RA3.2 - ML/AI-based solutions.** There have already been efforts of integrating ML and AI capabilities within clouds, such as Google's AlphaGo, Apple Siri, and Microsoft's Cortana. In the future, ML and DL techniques could revolutionize the ways of storing big data in the cloud, in the terms of computational costs and required hardware space. AI and ML solutions also have a huge potential in reinforcing the security and reliability of cloud solutions. Moreover, these technologies could prevent data loss by detecting data breaches in cloud storages [67].

**Threats:** T3.1.2 - Inadequate design and planning or incorrect adaptation, T3.2.1 - Interception of information, T3.2.2 - Unauthorized acquisition of information (data breach), T3.3.1 - Configuration poisoning, T3.3.2 - Business process poisoning, T3.4.3 - Malicious code/software/activity, T3.4.6 - Failures of business process, T3.4.7 - Code execution and injection (unsecured APIs), T3.4.9 - State-sponsored attacks, T3.5.1 - Violation of laws or regulations, T3.4.8 - Phishing - COVID-19, T3.6.5 - Cloud sprawl - COVID-19

**Gaps:** G3.6 - Gaps on forensics, G3.8 - Lack of visibility/control, G3.12 - Gaps on insider threat, G3.15 - Gaps on insecure interfaces and APIs

**RA3.3 - Data encryption.** Despite the continuous development of cloud environments and the emergence of upcoming technologies, the open nature of the cloud comes with risks. The introduction and deployment of new cloud-related technologies only exacerbate this risk, by introducing even more security holes. Encryption arises as one of the most appropriate solutions for these Gaps: However, currently available encryption technologies, as well intrusion detection systems are not sufficiently efficient in protecting large-scale systems such as clouds. Hence, there is a need to conduct further research in improving existing and developing new intrusion detection solutions and encryption techniques. Some of the potential solutions to these problems include real-time encryption technology [68], real-time defensive systems, and lightweight cryptographic solutions such as AES [69].

**Threats:** T3.2.1 - Interception of information, T3.2.2 - Unauthorized acquisition of information (data breach), T3.3.2 - Business process poisoning, T3.4.1 - Identity fraud, T3.4.5 - Misuse of assurance tools

**Gaps:** G3.1 - Gaps on the use of cryptography, G3.2 - Gaps on data control, G3.10 - Gaps on lack of cloud security architecture and strategy, G3.11 - Gaps on insufficient identity, credential, access, and key management, G3.15 - Gaps on insecure interfaces and APIs, G3.16 - Gaps on account hijacking due to the inadequate authentication, G3.18 - Gaps on malware exposure, G3.21 - Gaps on endpoint controls, G3.24 - Gaps on the configuration of cloud storage

**RA3.4 - Cloud-to-cloud backup.** Cloud-to-cloud backup is expected to become a standard procedure in the upcoming future<sup>58</sup>. It involves the process of backing-up data stored on one cloud onto another cloud. Current backup technologies deployed on the cloud are still susceptible to data loss due to hardware failures or natural disasters. Even though cloud-to-cloud technology could solve these issues, it is still in its infancy and requires more research to further bolster its security aspects and resolve other underlying issues, such as the clashes with other deduplication technologies.

**Threats:** T3.1.1 - Information leakage/sharing due to human errors, T3.2.2 - Unauthorized acquisition of information (data breach), T3.4.2 - Denial of service, T3.4.6 - Failures of business process, T3.4.9 – State-sponsored attacks, T3.6.2 - Malicious insider

**Gaps:** G3.13 - Gaps on weak control planes, 3.20 - Gaps on logistic challenges to the ever-increasing cloud usage, G3.24 - Gaps on the configuration of cloud storage

### Highlights on Identified Research Actions

There are four main areas in which future system cybersecurity research actions should be focused, namely SDN, ML/DL-based solutions, data encryption, and cloud-to-cloud backup. The efficiency of cloud services increased with the emergence of SDN-based cloud solutions, such as multi-clouds, hybrid clouds, meta-clouds, and clouds federations. Aside from being able to bring security standards to the next level by allowing network management from a single control panel, these solutions have the potential of differentiating good and malicious traffic.

ML and AI security solutions can be used not only for increasing the efficiency and reliability of cloud services but also for detecting data breaches in the cloud. Aside from bringing various benefits to the end-users, deployment of the emerging cloud-based technologies and add-ons usually introduces new security gaps and risks. Despite being one of the most suitable solutions for preventing such events, available data encryption solutions are not fully suitable for the clouds. Hence, there arises a need for new solutions and further research on novel concepts such as real-time encryption technology and real-time defensive systems. One of the most anticipated new security solutions is cloud-to-cloud backup, which is expected to fix the shortcomings of traditional backup technologies. However, it is still in its infancy and a lot of work remains to be done, in order to resolve the clashes with the existing deduplication technologies.

### 3.2.4. Data-Centric Security

Based on the discussion of respective countermeasures identified regarding Data-Centric Security, these are briefly evaluated and complemented with a description of research actions foreseen.

#### 3.2.4.1. Countermeasures

We provide an overview of existing countermeasures that focus on one or more threats, and address gaps and challenges in Appendix A.4. This section aims to present the status of

---

<sup>58</sup> Hot data storage technology trends for 2017, <https://searchstorage.techtarget.com/feature/Hot-data-storage-technology-trends-for-2017>

cybersecurity solutions connecting them to identified threats and gaps. We discuss classes of countermeasures, each describing the most relevant solutions to date.

**C4.1 - Identity Access Management.** Identity and Access Management (IAM) provides strategies and frameworks for managing digital identities. It enables IT, administrators, to control user access to sensitive data within organizations. Some of the technologies for IAM that enable secure storage and profiling of data and at the same time ensure enforcement of the required policies, include single sign-on systems, two-factor authentication, multi-factor authentication, privileged access management, etc. Additionally, organizations have to deploy authorization frameworks to provide only the required access rights to the users. Furthermore, automated tools and intermittent reviews should be utilized for reviewing and removing authorization rights from users that no longer need them<sup>59</sup>.

**Threats:** T4.2.2-Unauthorized acquisition of information (data breach), T4.3.1 - Data poisoning, T4.3.2 - Model poisoning, T4.4.1 - Identity fraud, T4.4.4 - Generation and use of rogue certificates, T4.4.5 - Misuse of assurance tools, T4.4.6 - Failures of business process, T4.4.9 – Extortion attacks, T4.5.1 - Violation of laws or regulations, T4.6.2 - Malicious insider

**Gaps:** G4.1 - Gaps on data protection, G4.5 - Gaps on data trustworthiness, G4.9 - Gaps on data management across borders, G4.10 - Gaps on the distributed data and frameworks

**C4.2 - Data masking and encryption.** Data masking enables end-users to create a faux version of the data that can be used for testing, training, processing, etc. Masked data keep their type, while its values get changed. That way real data is protected. Methods for data masking include encryption, character shuffling, and character/word substitution. End-users have to do the data masking in a way that its values cannot be reverse-engineered. Data encryption is critical for fulfilling the majority of the security strategies and compliance standards<sup>59</sup>.

**Threats:** T4.2.2 -Unauthorized acquisition of information (data breach), T4.3.1 - Data poisoning, T4.3.2 - Model poisoning, T4.4.6 - Failures of business process, T4.4.8 – Data extraction from ML models, T4.4.9 – Extortion attacks, T4.6.2 - Malicious insider

**Gaps:** G4.1 - Gaps on data protection, G4.2 - Gaps on the use of cryptography in applications and back-end data-intensive services, G4.11 - Gaps on the use of non-relational databases

**C4.3 - Anti-malware, antivirus, and endpoint protection.** Endpoint protection platforms combine antivirus tools with machine learning capabilities to detect abnormal behavior on the devices for detecting, never before seen attacks. Endpoint detection and response capabilities can aid in identifying data breaches on endpoints in real-time, enabling security teams to investigate them and lock affected endpoints promptly.

**Threats:** T4.2.1 - Interception of information, T4.2.2 -Unauthorized acquisition of information (data breach), T4.4.3 - Malicious code/software/activity, T4.4.7 - Code execution and injection (unsecured APIs), T4.4.9 – Extortion attacks

**Gaps:** G4.1 - Gaps on data protection, G4.9 - Gaps on data management across borders, G4.10 - Gaps on the distributed data and frameworks

**C4.4 - Data security auditing.** Security audits should be carried out periodically to identify potential gaps and vulnerabilities related to the organization. Security audits can be performed either by security experts from the organizations or by a third party (e.g. penetration testing model). Once the pertained security risks have been identified, organizations or end-users should invest available resources for resolving them<sup>59</sup>.

---

<sup>59</sup> What is Data Security?, <https://www.imperva.com/learn/data-security/data-security/>

**Threats:** T4.2.1 - Interception of information, T4.4.2 - Denial of service, T4.4.3 - Malicious code/software/activity, T4.4.6 - Failures of business process, T4.4.7 - Code execution and injection (unsecured APIs), T4.4.9 – Extortion attacks

**Gaps:** G4.6 - Gaps on decision support systems, G4.9 - Gaps on data management across borders, G4.11 - Gaps on the use of non-relational databases

**C4.5 - Enforcing password hygiene.** Having unique and strong passwords is one of the best ways to protect sensitive data. Unfortunately, the majority of the end-users jeopardize their sensitive information by using easily guessable weak passwords that can be broken with brute force attacks. The solution is enforcing multi-factor authentication that asks the user to identify themselves by token or fingerprints. Other solutions, such as the enforcement of longer passwords or enterprise password management systems come with security caveats for the organizations.

**Threats:** T4.1.1 - Information leakage/sharing due to human errors, T4.1.3 - Information leakage/sharing due to the hostile home network - COVID-19, T4.2.2 - Unauthorized acquisition of information (data breach), T4.4.1 - Identity fraud

**Gaps:** G4.1 - Gaps on data protection, G4.8 - Gaps in videoconferencing tools

**C4.6 - Data backups.** Creating backups of critical data or information in different locations is of high importance to aid in recovering from attacks that can tamper the data<sup>60</sup>. Apart from attacks, physical redundancy of data can also preserve it from natural disasters and sudden power outages. Periodically, it is also a good practice to audit backups and databases to find out who was trying to access the data<sup>61</sup>. For that matter and for enforcing data protection policies, data loss protection (DLP) software can be utilized, since it can alert administrators when large quantities of data are being copied outside the organization<sup>59</sup>.

**Threats:** T4.4.2 - Denial of service, T4.4.3 - Malicious code/software/activity, T4.4.6 - Failures of business process

**Gaps:** G4.1 - Gaps on data protection, G4.11 - Gaps on the use of non-relational databases

**C4.7 - Deployment of intrusion detection and prevention systems.** The distributed nature of big data opens door to intrusion attempts. Intrusion-detection systems (IDSs) can be set to check and collect data about potential attacks on database systems. Once the attack is identified by IDS, database administrators should be notified immediately. To further bolster protection against intrusions, intrusion prevention systems (IPS) should be deployed. Those systems enable security teams to safeguard big data platforms from weakness exploits by assessing network traffic. In most cases, IPS are set up behind firewalls and can therefore isolate intrusion before any damage is done. Moreover, IPS can be used to manage user privileges, for instance, denying access to certain resources.

**Threats:** T4.2.1 - Interception of information, T4.2.2 -Unauthorized acquisition of information (data breach), T4.4.2 - Denial of service, T4.4.3 - Malicious code/software/activity, T4.4.4 - Generation and use of rogue certificates, T4.4.5 - Misuse of assurance tools, T4.4.7 - Code execution and injection (unsecured APIs), T4.4.8 – Data extraction from ML models, T4.4.9 – Extortion attacks

**Gaps:** G4.6 - Gaps on decision support systems

**C4.8 - User awareness training and education.** Insufficient level of cybersecurity expertise and inadequate education of employees can lead to database breaches. Non-technical employees can jeopardize the database by not following the security rules. IT security personnel should undergo education and training for implementing security

---

<sup>60</sup> Cyber security: Threats, Vulnerabilities and Countermeasures -A Perspective on the State of Affairs in Mauritius,

[https://www.academia.edu/13578905/Cyber\\_security\\_Threats\\_Vulnerabilities\\_and\\_Countermeasures\\_A\\_Perspective\\_on\\_the\\_State\\_of\\_Affairs\\_in\\_Mauritius?auto=download](https://www.academia.edu/13578905/Cyber_security_Threats_Vulnerabilities_and_Countermeasures_A_Perspective_on_the_State_of_Affairs_in_Mauritius?auto=download)

<sup>61</sup> Database Security Threats And Countermeasures, <https://www.datasunrise.com/blog/potential-db-threats/database-security-threats-and-countermeasures/>

controls, enforcing policies, and conducting response processes, while the end-users should undergo basic training in database security. Finally, both IT professionals and end-users should strive to stay up-to-date with cybersecurity trends<sup>61</sup>.

**Threats:** T4.1.1 - Information leakage/sharing due to human errors, T4.1.2 - Inadequate design and planning or incorrect adaptation, T4.1.3 - Information leakage/sharing due to the hostile home network - COVID-19, T4.4.1 - Identity fraud, T4.4.9 – Extortion attacks, T4.5.1 - Violation of laws or regulations, T4.6.1 - Skill shortage

**Gaps:** G4.4 - Gaps on roles (skill shortage), G4.7 - Gaps on ethics, G4.8 - Gaps in videoconferencing tools

**C4.9 – Data poisoning detection.** It is possible to identify poisoning on the model level by comparing the output of a new version of a model to its previous iterations. The common attack technique is to provide the model training data with mislabelled entries to persuade the target function to shift its edge cases. Using large and fixed test sets it is possible to identify alteration in the behavior of the model, indicating a possible poisoning attack.

**Threats:** T4.3.1 - Data poisoning, T4.3.2 - Model poisoning

**Gaps:** G4.1 - Gaps on data protection, G4.3 - Gaps on computing and storage models and infrastructures, G4.11 - Gaps on the use of non-relational databases

### Highlights on Identified Countermeasures

IT administrators can use IAM to control user access to sensitive data inside organizations through techniques such as single sign-on systems, two-factor authentication, multi-factor authentication, and privileged access management. Data masking methods including encryption, character shuffling, and character/word substitution can enable users to protect their data by changing their values, while still keeping their type. Endpoint protection and response techniques are useful to identify data breaches in real-time and lock jeopardized endpoints. Data security audits have to be performed periodically by security experts to identify new gaps and weaknesses. Enforcing password hygiene practices such as using multi-factor authentication solutions is one of the best ways of protecting sensitive data. To alleviate the process of recovering from the potential attacks data backups of critical data should be deployed in different locations. IDSs and IPSs should be deployed for the collection of data containing information about the potential attacks, as well as for hardening protection against intrusions.

#### 3.2.4.2. Research Actions

We provide a discussion on relevant research actions that need to be taken to mitigate the threats, gaps, and challenges previously identified and reported in Appendix A.4.

**RA4.1 - Decentralized and blockchain-based solutions.** Even though it is still popular among some big companies, storing data in a centralized way, it renders it susceptible to the single point of failure and data breaches. To mitigate such issues, blockchain solutions can be utilized to move data from big data silos to distributed data storage. The combination of blockchain and big data can ensure the trustworthiness and integrity of generated data while reducing the likelihood of interference due to its known origin. This is attributed to the data immutability which is enabled by blockchain's consensus mechanism and secure hash functions [70]. Recently, there have been several endeavours in this big data security research area. Yue et al. [71] developed a credible platform based on blockchain and smart contracts for data sharing between data producers and customers. The authors utilized blockchain for ensuring data traceability and transparency, and smart contracts for ensuring

security while sharing data. Similarly, Xia et al. [72] proposed an auditing platform for controlling shared medical data in cloud repositories. The proposed platform enables data transferring between different sources in a tamper-resistant fashion. Uchibeke et al. [73] developed a blockchain access control ecosystem for managing access control of big data and safeguarding it against data breaches, while at the same time ensuring data auditability, transparency, and owner self-sovereignty. Moreover, the platform is also loosely based on Identity-Based Access Control (IBAC), and Role-Based Access Control (RBAC), and for each access control implementation features request, grant, revoke, verify, and view asset operations. Even though there is a continuously increasing number of research works on blockchain data security, there are still open challenges on decentralized and context-aware data warehousing that have to be solved.

**Threats:** T4.1.2 - Inadequate design and planning or incorrect adaptation, T4.2.2- Unauthorized acquisition of information (data breach), T4.2.3 - Conversation Eavesdropping/Hijacking - COVID-19, T4.4.2 - Denial of service, T4.4.6 – Failures of business processes, T4.5.1 - Violation of laws or regulations, T4.6.1 - Skill shortage

**Gaps:** G4.3 - Gaps on computing and storage models and infrastructures, G4.5 - Gaps on data trustworthiness, G4.6 - Gaps on decision support systems, G4.8 - Gaps in videoconferencing tools, G4.10 - Gaps on the distributed data and frameworks

**RA4.2 - Access control and data encryption.** Security issues may emerge during the transmission of big data to the cloud. To prevent data from ending up in the wrong hands, encryption and access control techniques arise as possible solutions. Moreover, transmission requires data to be decrypted, thus exposing it to security vulnerabilities. One of the common solutions involves data masking schemes. Several works proposed data encryption schemes based on Fully Homomorphic Encryption (FHE) [74] [75] [76]. Even though they achieved encryption before data transmission, the solution was limited only to numerical data. Other recent popular research efforts on data encryption involve work on improving ABE [77] and Format-preserving encryption techniques, as well as the development of novel lightweight schemes, such as Light-weight Encryption using Scalable Sketching (LESS) [78] which aimed to optimize and encrypt big data processing. There have been several research works on the access control and privacy of big data in recent times. Gupta et al. [79] proposed a big data compliance system for ensuring secure big data analysis in real-time dependent on its web directory and self-assurance framework for identifying genuine users. The framework proposed by Al-Shomrani et al. [80] utilizes techniques such as security policy manager, fragmentation approach, encryption approach, and security manager for analyzing and securing sensitive data received from the customers, while the work of Lee et al. [81] protects confidentiality and integrity of patients' private data through digital signature encryption and Diffie-Hellman session key. Even though not as popular as data encryption, access control solutions remain important in protecting big data security. Furthermore, this paper also includes experiments and computational verifications of the theory and proposed applications of this approach to science and technology, computer intelligence, and machine learning.

**Threats:** T4.1.1 - Information leakage/sharing due to human errors, T4.1.3 - Information leakage/sharing due to the hostile home network - COVID-19, T4.2.1 - Interception of information, T4.2.2-Unauthorized acquisition of information (data breach), T4.2.3 - Conversation Eavesdropping/Hijacking - COVID-19, T4.4.1 - Identity fraud, T4.4.9 – Extortion attacks

**Gaps:** G4.1 - Gaps on data protection, G4.2 - Gaps on the use of cryptography in applications and back-end data-intensive services, G4.8 - Gaps in videoconferencing tools, G4.9 - Gaps on data management across borders, G4.11 - Gaps on the use of non-relational databases

**RA4.3 - ML/AI-based solutions.** Unsupervised learning and deep learning algorithms such as clustering, linear regression, and neural networks have been successfully used for malware and intrusion detection. However, there are still challenges related to these techniques that have to be resolved when it comes to protecting big data. One such challenge is adaptability, which can be exploited by attackers in a way to trick the ML model to produce a different result. Until now the research efforts have focused on feature squeezing which focuses on reducing the search space available to attackers through merging samples related to multiple feature vectors into a single one [82] [83]. Similar issues are found in AI solutions, hence organizations and end-users should not consider ML nor AI as sole ways of defending against malware. The rise of Generative Adversarial Networks calls for combining both humans and AI in malware detection. In some other cases, data has to be protected from the people who work with it. Such situations require the complete removal of human intervention and the introduction of automation. One such solution was provided by Pissanetzky [84] who proposed a causal set as the universal language for all information for ML and computer intelligence applications.

**Threats:** T4.2.1 - Interception of information, T4.2.2-Unauthorized acquisition of information (data breach), T4.2.3 - Conversation Eavesdropping/Hijacking - COVID-19, T4.3.1 - Data poisoning, T4.3.2 - Model poisoning, T4.4.3 - Malicious code/software/activity, T4.4.5 - Misuse of assurance tools, T4.4.6 - Failures of business processes, T4.4.7 - Code execution and injection (unsecured APIs), T4.4.8 – Data extraction from ML models, T4.4.9 – Extortion attacks

**Gaps:** G4.1 - Gaps on data protection, G4.2 - Gaps on the use of cryptography in applications and back-end data-intensive services, G4.5 - Gaps on data trustworthiness, G4.6 - Gaps on decision support systems, G4.7 - Gaps on ethics

**RA4.4 - Self-destructing data.** The sheer amount of the recent data breaches resulted in establishing regulations such as the Breach of Security Safeguards Regulations and GDPR, which provides the ‘right to be forgotten’. This enables end-users to enforce the deletion of information related to them. To resolve data privacy issues, it is expected that future research will focus on self-destructing data solutions. One such research effort has already been conducted in the work of Geambasu et al. [85]. In their work authors proposed architecture that rendered copies of old privacy data obsolete and unable to surface. More research on this topic is expected to be conducted in the forthcoming future, but it will have to deal with the big data regulation challenges and policies [70].

**Threats:** T4.1.1 - Information leakage/sharing due to human errors, T4.1.3 - Information leakage/sharing due to the hostile home network - COVID-19, T4.2.2-Unauthorized acquisition of information (data breach), T4.3.3 - Unreliable data, T4.4.3 - Malicious code/software/activity, T4.4.9 – Extortion attacks, T4.6.2 - Malicious insider

**Gaps:** G4.1 - Gaps on data protection, G4.7 - Gaps on ethics

### **Highlights on Identified Research Actions**

There are four main areas in which future data cybersecurity research actions should focus, namely improving decentralized and blockchain-based solutions, access control and data encryption solutions, ML/AI-based solutions, and solutions including self-destructing data. Blockchain solutions can be used to move data from big data warehouses to distributed storage, thus eliminating the risks of data breaches and single points of failure. Moreover, blockchain’s immutability property can grant trustworthiness, auditability, transparency, and integrity of big data. Encryption and access control remain powerful solutions in ensuring security during big data transmissions to the cloud. Popular recent data encryption solutions include data masking schemes, Fully Homomorphic Encryption (FHE), lightweight cryptography variations, and improvements of techniques such as ABE.

Unsupervised learning and deep learning algorithms have been used for malware and intrusion detection fairly successfully during the past few years. Current research efforts in this area focus mostly on feature squeezing to reduce the research space available to potential adversaries. One of the main challenges of ML solutions lies in adaptability, through which adversaries can trick the ML model into producing wrong results. A large number of recent data breaches have inspired the establishment of regulations that enable end-users to enforce information deletion. Consequently, future research should focus on developing reliable self-destructing data solutions with privacy in mind. Finally, increasing the robustness of ML models at both training and inference time is fundamental to strengthen modern distributed systems against training poisoning and adversarial attacks.

### 3.2.5. Application-Centric Security

Based on the discussion of respective countermeasures identified regarding Application-Centric Security, these are briefly evaluated and complemented with a description of research actions foreseen.

#### 3.2.5.1. Countermeasures

We provide an overview of existing countermeasures that focus on one or more threats, and address gaps and challenges in Appendix A.5. This section aims to present the status of cybersecurity solutions connecting them to identified threats and gaps. We discuss classes of countermeasures, each describing the most relevant solutions to date.

**C5.1 - Security by default.** It refers to the technologies which enable security best practices by default, requiring little to no manual intervention. They help in solving all those long-standing issues and threats which are widely known but still largely exploited. There are many security-by-default techniques that can be applied at different levels, including the following ones. At the low level, programming language compilers that add safety and security features (*e.g.*, buffer overflow protection) to the compiled code are used in many modern programming languages (*e.g.*, Java, Python), with built-in dynamic analysis tools (*e.g.*, fuzzing in Go),<sup>62</sup> offering in some cases very strong guarantees (*e.g.*, memory safety at compile time in the case of Rust).<sup>63</sup> Moving up on the stack, modern web frameworks offer protection from common threats such as SQL Injection,<sup>64</sup> XSS (Cross-Site Scripting). At a high level, orchestration platforms (*e.g.*, Docker Swarm, Kubernetes) offer SDNs (Software Defined Networks) with many security features, including automatic encryption and mutual authentication (see C5.3).<sup>65,66</sup> The key point that makes these solutions a step forward is that they require very little effort to set up their security and safety features. Some of them even aim to provide security features without modifying the application code. In fact, security by default is fundamental in a scenario where 65% of publicly disclosed cloud security incidents are the result of cloud customer misconfigurations.<sup>67</sup>

---

<sup>62</sup> The Go Blog. Fuzzing is Beta Ready. <https://blog.golang.org/fuzz-beta>

<sup>63</sup> Microsoft Security Response Center. Why Rust for safe systems programming. <https://msrc-blog.microsoft.com/2019/07/22/why-rust-for-safe-systems-programming/>

<sup>64</sup> Spring Javadoc. Class NamedParameterJdbcTemplate. <https://docs.spring.io/spring-framework/docs/5.3.0/javadoc-api/index.html?org/springframework/jdbc/core/namedparam/NamedParameterJdbcTemplate.html>

<sup>65</sup> Docker. Use overlay networks. <https://docs.docker.com/network/overlay/#encrypt-traffic-on-an-overlay-network>

<sup>66</sup> Istio. Security. <https://istio.io/latest/docs/concepts/security/>

<sup>67</sup> Palo Alto Unit 42. Cloud Threat Report 1H 2021

**Threats:** T5.1.1 - Security misconfiguration, T5.2.1 - Interception of information, T5.2.2 - Sensitive data exposure, T5.3.1 - Broken authentication and access control, T5.3.3 - Code execution and injection (unsecured APIs), T5.3.6 - Supply-chain security, T5.3.8 – Source code breach

**Gaps:** G5.1 - Gaps on microservice-aware security, G5.2 - Gaps on authentication and authorization, G5.3 - Gaps on orchestration and composition, G5.4 - Gaps on safety and security by default, G5.5 - Gaps on the proper management of configurations, G5.6 - Gaps on supply-chain security, G5.7 - Gaps on skills

**C5.2 - Authentication and Authorization.** It refers to the activities where the user who wants to access a resource is first identified (authentication) and then, eventually, authorized (authorization). Recent advances in threats paired with the long-standing issue of weak passwords call for new methods for authentication and authorization. On one side, MFA (Multi-Factor Authentication) is becoming the go-to technology to improve authentication. On the other side, advanced paradigms began to be used outside of research (*e.g.*, attribute-based access control). If applied correctly, *e.g.*, the two-men rule, they can partially mitigate threats such as malicious insiders. However, the complexity of such solutions is also increasing, and designers and implementers must make careful choices to avoid opening up for new threats. We note that in microservice and distributed systems, authentication and authorization is performed directly from service to service, hence the concept of *users* may not be enough.<sup>68</sup>

**Threats:** T5.1.2 - Inadequate design, T5.2.2 - Sensitive data exposure, T5.3.1 - Broken authentication and access control, T5.5.1 - Malicious insider

**Gaps:** G5.1 - Gaps on microservice-aware security, G5.2 - Gaps on authentication and authorization, G5.4 - Gaps on safety and security by default, G5.7 - Gaps on skills, G5.9 - Gaps on education, G5.10 - Gaps on sophisticated protection

**C5.3 - Orchestration Platforms.** They refer to the very fundamental requirement for every system based on containers. Orchestration platforms such as *Kubernetes* enable automatic deployment, resource management, scaling, and programming patterns required to write the very minimum amount of code (serverless). Beyond that, they provide a set of ready-to-use building blocks that can help solve many use cases, either as built-in or as add-ons. Among them, comprehensive and monitoring solutions (*e.g.*, *OpenTelemetry*<sup>69</sup>), layer-7 security solutions eventually the basis of C5.2 (*e.g.*, *Cilium*<sup>70</sup>), container-native threat detection (*e.g.*, *Falco*<sup>71</sup>). In short, orchestration platforms can greatly simplify many common tasks, some of them related to security. Nevertheless, as specified in deliverable D4.2, they may have vulnerabilities themselves and require mastering many concepts. This countermeasure is related to C5.1, *i.e.*, such platforms should in any case be secure by default. Finally, they can be often paired with tools to automate configurations and deployments aimed at reducing human errors (*e.g.*, IaC – Infrastructure as Code).<sup>72,73,67</sup>

**Threats:** T5.1.1 - Security misconfiguration, T5.1.2 - Inadequate design, T5.2.1 - Interception of information, T5.2.2 - Sensitive data exposure, T5.3.1 - Broken authentication and access control, T5.3.2 - Denial of service, T5.3.3 - Code execution and injection (unsecured APIs), T5.3.4 - Insufficient logging and monitoring, T5.3.5 - Untrusted composition, T5.3.7 - Virtualization

<sup>68</sup> Istio. Security - Authentication. <https://istio.io/latest/docs/concepts/security/#authentication>

<sup>69</sup> OpenTelemetry. <https://opentelemetry.io/>

<sup>70</sup> Cilium. <https://cilium.io/>

<sup>71</sup> Falco. <https://falco.org/>

<sup>72</sup> Palo Alto Unit 42. Cloud Threat Report 1H 2021

<sup>73</sup> Microsoft. What Is Infrastructure as Code? <https://docs.microsoft.com/en-us/devops/deliver/what-is-infrastructure-as-code>

**Gaps:** G5.1 - Gaps on microservice-aware security, G5.2 - Gaps on authentication and authorization, G5.3 - Gaps on orchestration and composition, G5.4 - Gaps on safety and security by default, G5.5 - Gaps on the proper management of configurations, G5.7 - Gaps on skills, G5.10 - Gaps on sophisticated protection

**C5.4 - Sandboxing.** It refers to the techniques isolating (a set of) processes, often aiming at reducing attack spreading and failures. In a nutshell, the principle is to make the running process unable to escape the sandbox for none but the allowed actions. The gold standard for sandboxing is containerization, a lightweight virtualization technology (*i.e.*, *Docker*). Recently, another promising technology is *WebAssembly*, an assembly-like language born to speed up client-side Javascript. *WebAssembly* is rapidly gaining attention also for server-side execution, with *WebAssembly* runtimes offering built-in sandboxing.<sup>74</sup> Many compilers are adding *WebAssembly* as a target, and some providers are offering *WebAssembly*-based hosting platforms.<sup>75</sup> In short, it is becoming a revival of the old motto “write once, run anywhere”, but in a multi-language fashion. In fact, these kinds of sandboxing (*i.e.*, containers and *WebAssembly*), favour also portability; but threat actors are already maliciously exploiting them for, *e.g.*, obfuscation.<sup>76</sup>

**Threats:** T5.1.1 - Security misconfiguration, T5.1.2 - Inadequate design, T5.3.3 - Code execution and injection (unsecured APIs), T5.3.7 – Virtualization, T5.3.8 – Source code breach

**Gaps:** G5.1 - Gaps on microservice-aware security, G5.4 - Gaps on safety and security by default, G5.6 - Gaps on supply-chain security, G5.7 - Gaps on skills, G5.8 - Gaps on interoperability

### Highlights on Identified Countermeasures

The above countermeasures consider two main directions: *i*) simplifying the security-related maintenance burden on developers and IT admins; *ii*) providing improved protection. The recent years have seen the trends of shifting security “to the left”, culminating in the definition of development methodologies such as DevSecOps.

In short, they advocate for the early inclusion of security in the development process, making it one of the pillars guiding all the choices. In this context, solutions that are already secure or safe play a crucial role, reducing the efforts both of developers and system administrators. They greatly help in removing many long-standing issues still affecting the security landscape,<sup>77</sup> allowing personnel to focus on sophisticated security aspects. In other words, existing countermeasures are forming the basis on which more sophisticated solutions should be built.

#### 3.2.5.2. Research Actions

We provide a discussion on relevant research actions that need to be taken to mitigate the threats, gaps, and challenges previously identified and reported in Appendix A.5. As cyber-hygiene practices are improving, threat actors rely more and more on two main aspects to

---

<sup>74</sup> Wasmer. <https://wasmer.io/>

<sup>75</sup> Cloudflare Workers. Languages. <https://developers.cloudflare.com/workers/platform/languages#wasm-supported>

<sup>76</sup> M. Musch C. Wressnegger, M. Johns, K. Rieck. "New Kid on the Web: A Study on the Prevalence of *WebAssembly* in the Wild". In Proc of DIMVA 2019. Gothenburg, Sweden

<sup>77</sup> OWASP Top Ten 2017. <https://owasp.org/www-project-top-ten/2017/>

successfully carry their attacks: *i)* human factor;<sup>78 79</sup> *ii)* supply-chain.<sup>80</sup> These are the two main areas that research should focus on.

**RA5.1 - Zero Trust (ZT) security.** It is a paradigm where, in short, *everything is considered malicious and untrusted*. It moves from implicitly trusting assets because of their location (*e.g.*, intranet) or ownership, towards a dynamic approach where authentication and authorization are explicitly granted.<sup>81</sup> It can be seen as an enhancement of Security by default (C5.1). We note that ZT is a set of guidelines to apply organization-wide, and it is critically important considering the actual trends towards *hybrid* architectures (*i.e.*, cloud, edge, IoT, BYOD, remote work). The ideas behind ZT seem to be understood and promising, and some production-ready solutions begin to emerge,<sup>82</sup> despite ZT being still in an early stage. There are many aspects to investigate, for instance, *i)* impact evaluation, *i.e.*, how existing practices change in a ZT architecture; *ii)* effective migration strategies, to name but a few.

**Threats:** T5.1.1 - Security misconfiguration, T5.1.2 - Inadequate design, T5.2.1 - Interception of information, T5.2.2 - Sensitive data exposure, T5.3.1 - Broken authentication and access control, T5.3.2 - Denial of service, T5.3.3 - Code execution and injection (unsecured APIs), T5.3.5 - Untrusted composition, T5.3.6 - Supply-chain security, T5.5.1 - Malicious insider

**Gaps:** G5.1 - Gaps on microservice-aware security, G5.2 - Gaps on authentication and authorization, G5.3 - Gaps on orchestration and composition, G5.4 - Gaps on safety and security by default, G5.5 - Gaps on the proper management of configurations, G5.6 - Gaps on supply-chain security, G5.7 - Gaps on skills, G5.9 - Gaps on education, G5.10 - Gaps on sophisticated protection

**RA5.2 - AI/ML for Security.** It refers to the use of Artificial Intelligence in the context of security. AI is now capable of solving tasks of huge complexity, from image recognition to text generation. It can play a crucial role in improving security, especially addressing those problems for which traditional approaches have well-known limitations, *e.g.*, IDS, traffic analysis. In the application domain, AI can help in many ways, for instance, code analysis (*e.g.*, to recognize malicious apps whose code is obfuscated), continuous authentication, application, and user monitoring, to name but a few. In parallel, it is fundamental to understand (*i)* the novel challenges AI brings; (*ii)* the limitations of such approaches, for instance, there are already cases when ML-based detection tools are being bypassed;<sup>83</sup> (*iii)* how AI can be used to cause damage, either voluntary or not.

**Threats:** T5.2.1 - Interception of information, T5.2.2 - Sensitive data exposure, T5.3.2 - Denial of service, T5.3.6 - Supply-chain security, T5.5.1 - Malicious insider

**Gaps:** G5.2 - Gaps on authentication and authorization, G5.6 - Gaps on supply-chain security, G5.10 - Gaps on sophisticated protection

**RA5.3 - Authentication.** It refers to novel forms of sophisticated authentication, which, in its basic form is already a countermeasure (C5.2). Today, MFA is strongly recommended to overcome the issues of weak passwords. However, many MFA systems are only a second

---

<sup>78</sup> Blackberry 2021 Threat Report.

<sup>79</sup> Accenture. Cyber Threatscape Report. 2019.

. <https://www.accenture.com/acnmedia/pdf-107/accenture-security-cyber.pdf>

<sup>80</sup> Accenture. Cyber Treatscape Report. 2020.

<sup>81</sup> NIST SP 800-207. Zero Trust Architecture. 2020. <https://csrc.nist.gov/publications/detail/sp/800-207/final>

<sup>82</sup> Istio. Security. <https://istio.io/latest/docs/concepts/security/>

<sup>83</sup> Sophos 2021 Threat Report. <https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf>

layer over passwords.<sup>84</sup> Furthermore, MFA systems are typically complex to set up, because they require supporting infrastructure and policies to deal with devices loss, SIM hijacking threats, etc.<sup>8586</sup> Rather, novel authentication solutions should be “purely passwordless”, *i.e.*, not requiring passwords at all. To this aim, biometric authentication is acknowledged as the most secure way of authentication, followed by token-based approaches (*e.g.*, apps installed on a device). Still, these methods have their challenges. For instance, biometrics *i)* often relies on specialized hardware; *ii)* faces harsh criticisms, as, in some cases, it is perceived as a form of mass surveillance. In this sense, research on authentication should focus on the *integration* and the *applicability* of passwordless authentication in wider and much complex architectures, while strictly adhering to privacy requirements.

**Threats:** T5.1.2 - Inadequate design, T5.2.2 - Sensitive data exposure, T5.3.1 - Broken authentication and access control, T5.3.8 – Source code breach

**Gaps:** G5.1 - Gaps on microservice-aware security, G5.2 - Gaps on authentication and authorization, G5.4 - Gaps on safety and security by default, G5.7 - Gaps on skills, G5.9 - Gaps on education, G5.10 - Gaps on sophisticated protection

**RA5.4 - Supply-Chain.** It refers to the security of all the components (*e.g.*, hardware, libraries) of an application or an ICT product. In general, attackers are shifting towards *indirect* attacks, exploiting the supply chain (and the human factor as well).<sup>87</sup> A typical example of that kind of exploitation was the case of SolarWinds<sup>88</sup>, one of the most severe attacks recently happened. Supply-chain attacks are often distributed through software updates. For this reason, research in this field, should address also the long-standing issue of patch management, for instance how to effectively update the plethora of devices forming IoT,<sup>89909192</sup> and to avoid the update mechanism being a threat itself<sup>93</sup>. There are projects explicitly aimed at securing updates (*e.g.*, TUF<sup>94</sup>). However, little research has been devoted to properly addressing supply-chain security as a whole in IT, while it has been investigated in other domains. In general, the supply chain is often related to the concept of risk and trust. Hence, some authors are advocating for supply chain management following the Zero Trust principles.<sup>95</sup>

**Threats:** T5.1.2 - Inadequate design, T5.2.2 - Sensitive data exposure, T5.3.1 - Broken authentication and access control, T5.3.3 - Code execution and injection (unsecured APIs),

---

<sup>84</sup> Gartner. Top Security and Risk Management Trends. 2019

<sup>85</sup> Gartner. Top security and risk management trends for 2021

<sup>86</sup> Sophos Threat Report 2020, <https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-uncut-2020-threat-report.pdf>

<sup>87</sup> Accenture. Third Annual State of Cyber Resilience. 2020. <https://www.accenture.com/acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf>

<sup>88</sup> CSO. SolarWinds attack explained: And why it was so hard to detect.

<https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html>

<sup>89</sup> JSOF. Ripple20. <https://www.jsf-tech.com/disclosures/ripple20>

<sup>90</sup> Wired. An Operating System Bug Exposes 200 Million Critical Devices.

<https://www.wired.com/story/vxworks-vulnerabilities-urgent11/>

<sup>91</sup> Wired. Decades-Old Code Is Putting Millions of Critical Devices at Risk.

<https://www.wired.com/story/urgent-11-ipnet-vulnerable-devices/>

<sup>92</sup> Armis. URGENT/11 Affects non-Vxworks Operating Systems. <https://www.armis.com/blog/urgent11-affects-additional-rtoss-highlights-risks-on-medical-devices/>

<sup>93</sup> Wired. This Bluetooth Attack Can Steal a Tesla Model X in Minutes. <https://www.wired.com/story/tesla-model-x-hack-bluetooth/>

<sup>94</sup> TUF - The Update Framework. <https://theupdateframework.io>

<sup>95</sup> The zero trust supply chain: Managing supply chain risk in the absence of trust. Zachary A. Collier, Joseph Sarkis. International Journal of Production Research. 2021.

<https://www.tandfonline.com/doi/full/10.1080/00207543.2021.1884311>

T5.3.5 - Untrusted composition, T5.3.6 - Supply-chain security, T5.3.7 – Virtualization, T5.3.8 – Source code breach

**Gaps:** G5.3 - Gaps on orchestration and composition, G5.4 - Gaps on safety and security by default, G5.6 - Gaps on supply-chain security

### Highlights on Identified Research Actions

The above research actions point to the definition of sophisticated forms of security, built on solid ground. This ground consists of ZT enhancing security by default (C5.1), where the physical network perimeter no longer coincides with the logical security perimeter, an approach pioneered by Google, among the others.<sup>96</sup> One of the fundamental pillars of ZT is *identity*<sup>97</sup>, as it is often the only barrier to obtain access to resources. Clearly, it requires strong forms of authentication, possibly token-based or biometric, or, in any case, beyond passwords. We note that, as already mentioned in R5.3, this brings in new layers of complexity that are not easy to cope with, especially for small and medium-sized organizations.

Next, AI can improve the state of the art in many sectors where, for instance, classification tasks are required. However, AI by itself is not the cure-all solution, and organizations need to strongly think about the implications of AI and its notorious unpredictable behavior. Finally, as attacks are increasingly indirect, supply-chain security should be properly investigated. In general, securing the software supply chain is not an easy task as it involves a thorough knowledge of the whole chain.

#### 3.2.6. User-Centric Security

Based on the discussion of respective countermeasures identified regarding User-Centric Security, these are briefly evaluated and complemented with a description of research actions foreseen.

##### 3.2.6.1. Countermeasures

We provide an overview of existing countermeasures that focus on one or more threats, and address gaps and challenges in Appendix A.6. This section aims to present the status of cybersecurity solutions connecting them to identified threats and gaps. We discuss classes of countermeasures, each describing the most relevant solutions to date.

**C6.1 – Security training.** A solid security training may prevent many incidents, reducing significantly the risks associated with user-centric threats. Most attacks focus on gaps that are easily avoidable by providing basic security training to the users, allowing them to understand the implications of their actions in an organization. Examples of fields of training include password handling, identification of frauds (*e.g.*, phishing emails), network security (*e.g.*, encryption, VPNs, trusted sources), social engineering techniques. More focused training should be introduced into software engineering-related roles.

**Threats:** T6.1.1 - Mishandling of physical assets, T6.1.2 - Misconfiguration of systems, T6.1.3 - Loss of CIA on data assets, T6.2.2 - Illegal acquisition of information, T6.3.1 -

---

<sup>96</sup> Rory Ward and Betsy Beyer. BeyondCorp: A New Approach To Enterprise Security. ;login:, vol 39 n 6. 2014.

[https://www.usenix.org/system/files/login/articles/login\\_dec14\\_02\\_ward.pdf](https://www.usenix.org/system/files/login/articles/login_dec14_02_ward.pdf)

<sup>97</sup> Gartner. Top security and risk management trends for 2021

Organized criminal groups' activity, T6.4.1 - Misinformation/disinformation campaigns, T6.5.1 - Skill shortage/undefined cybersecurity curricula, T6.5.3 - Pivoting

**Gaps:** G6.1 - Gaps on modelling user behavior, G6.2 - Gaps on the relation between user behavior and adverse security-related effects, G6.3 - Gaps on security information, G6.4 - Gaps on security training and education, G6.6 - Gaps on protection from online scammers

**C6.2 – Assessment of security standards implementation.** Security standards identify sets of rules and processes that grant quality and safety to the organizations that adopt them. Correct implementation of standards is a prerequisite, for their benefit to express, therefore it is advisable, to include assessment of their implementations in the organization processes.

**Threats:** T6.1.2 - Misconfiguration of systems, T6.4.2 - Smear campaigns/market manipulation, T6.5.1 - Skill shortage/undefined cybersecurity curricula, T6.5.2 - Business misalignment/shift of priorities

**Gaps:** G6.2 - Gaps on the relation between user behavior and adverse security-related effects, G6.4 - Gaps on security training and education

**C6.3 – Data encryption.** Encryption is a fundamental technique to preserve the confidentiality of information. The usage of a solid cryptographic system allows its users to exchange or store data in a privacy-preserving manner, even in adverse situations. Common methods for private network communications include VPNs, HTTPS, SOCKS5, PGP. Cryptographic techniques are effective as long as the encryption keys are not disclosed, therefore safe key and password management are prerequisites.

**Threats:** T6.1.1 - Mishandling of physical assets, T6.1.3 - Loss of CIA on data assets, T6.2.1 - Profiling and discriminatory practices, T6.2.2 - Illegal acquisition of information, T6.3.1 - Organized criminal groups' activity

**Gaps:** G6.2 - Gaps on the relation between user behavior and adverse security-related effects

**C6.4 – Access control policies.** Access control policies are sets of rules that allow identifying the subset of assets to which a certain user should be granted access. This kind of policy can be used to restrict the capabilities of users to the smallest number of systems or resources necessary for their tasks to be completed, reducing the risk of their misuse. Access control systems can automate this selection, based on the assigned tasks or the role inside the organization.

**Threats:** T6.1.3 - Loss of CIA on data assets, T6.2.2 - Illegal acquisition of information, T6.3.3 - Malicious employees or partners' activity, T6.5.3 - Pivoting

**Gaps:** G6.2 - Gaps on the relation between user behavior and adverse security-related effects, G6.4 - Gaps on security training and education, G6.5 - Gaps in collaborative protocols for disclosure

**C6.5 - Increase awareness on security and technology use.** Deep fakes, propaganda, misinformation, and disinformation campaigns are everywhere, designed to lead users into making mistakes. These social engineering campaigns have a direct impact on users' daily life and society. The only remedy not to fall into these trivial scams, and not to be influenced by bogus information, is to deeply inquire and research, on different sources, especially institutional ones. Recognizing how this information is used for social engineering is vital for security awareness training.

Awareness of what is happening around us, and the knowledge of the threat itself, are the only remedies to avoid information fraudsters.

**Threats:** T6.4.1 - Misinformation/disinformation campaigns, T6.4.2 - Smear campaigns/market manipulation, T6.4.3 - Social responsibility/ethics-related incidents, T6.5.1 - Skill shortage/undefined cybersecurity curricula

**Gaps:** G6.1 - Gaps on modelling user behavior, G6.2 - Gaps on the relation between user behavior and adverse security-related effects, G6.4 - Gaps on security training and education, G6.6 - Gaps on protection from online scammers

**C6.6 – Multi-factor authentication.** Multi-factor authentication is a technique of access control that validates a user identity using two or more authentication factors. These may include passwords, physical tokens (i.e., USB keys), software tokens (i.e. code generator), and biometric features (i.e. fingerprints, retina, behavior). Multi-factor authentication requires accessing users' multiple proofs of their identity, drastically reducing the likelihood of identity fraud.

**Threats:** T6.1.1 - Mishandling of physical assets, T6.3.1 - Organized criminal groups' activity

**Gaps:** G6.2 - Gaps on the relation between user behavior and adverse security-related effects

**C6.7 – Firewall.** Firewalls are the first line of defense for an organization's activity in a network and can be used to monitor and filter possibly malicious traffic. On the user level, a correctly configured firewall may detect and mitigate a large set of security risks, including phishing attacks, information leaks, incorrect network configurations, malicious code execution, and propagation.

**Threats:** T6.3.1 - Organized criminal groups' activity, T6.3.2 - State-sponsored organizations' activity

**Gaps:** G6.1 - Gaps on modelling user behavior

**C6.8 – Traffic analysis.** Traffic analysis consists of the monitoring of network traffic and the extraction of structured information. The acquired data can be used for further analysis, i.e. identifying patterns, inferencing the communication actors and the software used, etc. This kind of technique can be combined with firewalls and other tools to effectively identify abnormal or malicious traffic in an organization's network.

**Threats:** T6.3.1 - Organized criminal groups' activity, T6.3.2 - State-sponsored organizations' activity

**Gaps:** G6.1 - Gaps on modelling user behavior

**C6.9 - Tokens leaks prevention and mitigation.** Authentication tokens and secret keys often follow standardized text or binary formats. By analyzing network traffic, source code repositories, and logs, it is possible to identify accidentally leaked tokens, thus preventing their leak or automating their deactivation, alerting the relevant users. Examples of leaked tokens that can be detected are cloud platforms authentication tokens, SSH or VPNs private keys, clear text passwords.

**Threats:** T6.1.3 - Loss of CIA on data assets, T6.2.2 - Illegal acquisition of information

**Gaps:** G6.1 - Gaps on modelling user behavior, G6.2 - Gaps on the relation between user behavior and adverse security-related effects

**C6.10 – Log analysis.** The automated collection and analysis of systems logs is an effective technique to identify possible anomalies in an organization's systems. A log analysis process may detect malicious or erroneous behavior of users and services, providing an effective source of information for automated decision and defense systems.

**Threats:** T6.3.1 - Organized criminal groups' activity, T6.3.3 - Malicious employees or partners' activity

**Gaps:** G6.1 - Gaps on modelling user behavior, G6.4 - Gaps on security training and education

**C6.11 – Code analysis.** Various analysis techniques can be applied to code and configurations to prevent or mitigate human error. The static analysis uses abstraction over structured languages to infer and validate bounds and can identify logical errors. Dynamic analysis techniques are applied to running code and allow to verify its correctness. Fuzzing methods may be used to test execution paths against potentially malicious input.

**Threats:** T6.1.2 - Misconfiguration of systems

**Gaps:** G6.1 - Gaps on modelling user behavior, G6.4 - Gaps on security training and education

**C6.12 – Legal audit.** Legal threats are specific to the local legislation and the organization's internal rules. Users may not have a complete understanding of the legal aspects of their actions and possibly increase legal risks. A legal audit may analyze the internal processes, evaluate risks and identify specific countermeasures or mitigations.

**Threats:** T6.1.4 - Legal, reputational, and financial cost, T6.2.1 - Profiling and discriminatory practices, T6.3.3 - Malicious employees or partners' activity, T6.4.2 - Smear campaigns/market manipulation, T6.4.3 - Social responsibility/ethics-related incidents

**Gaps:** G6.3 - Gaps on security information, G6.5 - Gaps in collaborative protocols for disclosure

**C6.13 – Honeypots.** Honeypots are systems designed as baits for possible attackers. These machines are intentionally vulnerable systems, isolated from the production environment. They are heavily monitored, to observe and classify attacks against the organization network as a means to develop countermeasures against attacks to the main network. This kind of system can also be applied as an expedient against malicious insiders and pivoting, possibly simplifying the process of identification of the attacker.

**Threats:** T6.3.1 - Organized criminal groups' activity, T6.5.3 - Pivoting

**Gaps:** G6.1 - Gaps on modelling user behavior, G6.4 - Gaps on security training and education

### Highlights on Identified Countermeasures

Dealing with user-level security, requires considering both external and internal threats. The countermeasures listed above have been chosen with the intent of minimizing the security risks set by the threats indicated in Table 18 while being generalized to most organizations. Automated tools, like firewalls and traffic analysis, can be adopted to prevent external attacks. Internal attacks can be identified by monitoring network and execution logs, while their mitigation can be achieved using access control policies, roles separation, multi-factor authentication, and encryption. Depending on the organization's internal processes, more specific techniques can be integrated. Although the countermeasures indicated may reduce the risks, humans are still the weak link in the chain, therefore security training should be considered a basic prerequisite.

#### 3.2.6.2. Research Actions

We provide a discussion on relevant research actions that need to be taken to mitigate the threats, gaps, and challenges previously identified and reported in Appendix A.6.

**RA6.1 – Security training techniques.** Many devastating cyberattacks have been possible thanks to the lack of basic security training of organizations' and firms' personnel. Led by a false perception of the value of internal assets and the risks involved, the users tend to neglect their work environment safety and expose the organization and themselves to simple yet effective attacks. Effective security training should consider not only the technical aspects of the field but also the psychological and human nature of the trainees. Research on these themes is expected to identify more effective ways of teaching how to prevent security risks.

**Threats:** T6.1.1 - Mishandling of physical assets, T6.1.2 - Misconfiguration of systems, T6.1.3 - Loss of CIA on data assets, T6.2.2 - Illegal acquisition of information, T6.5.1 - Skill shortage/undefined cybersecurity curricula, T6.5.3 – Pivoting

**Gaps:** G6.1 - Gaps on modelling user behavior, G6.2 - Gaps on the relation between user behavior and adverse security-related effects, G6.3 - Gaps on security information, G6.4 - Gaps on security training and education, G6.6 - Gaps on protection from online scammers

**RA6.2 – Fight against disinformation.** The increasingly concerning spread of disinformation through online means has shown tangible effects on sensitive topics, including politics, health, and discrimination. Disinformation may be carried out by various users with diverse intentions and motives, among which terrorism and propaganda. Fleets of human or automated operated accounts have been capable of shifting the outcome of national elections, instigating large violent events, and propagating forged information discrediting health organizations. Research directions in countering disinformation include adversarial techniques against the spread of conspiracy theories; monitoring and identification of the sources of disinformation and conspiracy trends; development and spread of a correct fact-checking culture through a network of national and international institutions; detection and mitigation of forgery techniques, like deep fakes.

**Threats:** T6.2.1 - Profiling and discriminatory practices, T6.4.1 – Misinformation/disinformation campaigns, T6.4.2 - Smear campaigns/market manipulation, T6.4.3 - Social responsibility/ethics-related incidents, T6.5.1 - Skill shortage/undefined cybersecurity curricula

**Gaps:** G6.3 - Gaps on security information, G6.4 - Gaps on security training and education, G6.6 - Gaps on protection from online scammers

**RA6.3 – Social engineering and user behavior.** Social engineering attacks are still the most effective attacks against untrained users. The attacker may exploit gaps in the technical preparation, social and hierarchical assumptions and stressful situations to exploit users and gain access to assets of the organization or higher interest targets. Social engineering techniques may include both network-based attacks, like phishing and social network influence, and in-loco attacks. Research in social engineering and user behavior would allow to better profile the limitations of users against an experienced attacker and characterize methodologies to mitigate the associated risks.

**Threats:** T6.1.3 - Loss of CIA on data assets, T6.1.4 - Legal, reputational, and financial cost  
T6.2.2 - Illegal acquisition of information, T6.3.1 - Organized criminal groups' activity, T6.3.2 - State-sponsored organizations' activity, T6.3.3 - Malicious employees or partners' activity, T6.5.1 - Skill shortage/undefined cybersecurity curricula, T6.5.3 - Pivoting

**Gaps:** G6.1 - Gaps on modelling user behavior, G6.2 - Gaps on the relation between user behavior and adverse security-related effects, G6.4 - Gaps on security training and education, G6.6 - Gaps on protection from online scammers

**RA6.4 – AI applications for user security.** Machine learning and AI-based techniques have increasingly large fields of application and are particularly effective in complex environments, like user interactions, where a complete definition of the tackled problem is impossible. This research can be applied to user security, *i.e.*, to characterize users' behavior, detect anomalies, analyze network traffic, provide automatic decision making, improve authentication techniques, etc. More advanced techniques include user identification through biological features, automatic source code, and software analysis and security automation. The expansion of this field of research is now even more necessary as attackers are adopting ML-based attacks.

**Threats:** T6.1.2 - Misconfiguration of systems, T6.1.3 - Loss of CIA on data assets, T6.2.2 - Illegal acquisition of information, T6.3.1 - Organized criminal groups' activity, T6.3.2 - State-sponsored organizations' activity, T6.5.1 - Skill shortage/undefined cybersecurity curricula, T6.5.3 - Pivoting

**Gaps:** G6.1 – Gaps on modelling user behavior, G6.2 – Gaps on the relation between user behavior and adverse security-related effects, G6.4 – Gaps on security training and education

## Highlights on Identified Research Actions

The importance of research in the field of users' security is ever increasing in an age where information and privacy are the most valuable assets. The advancement of the base level of security training is an effective means of mitigating a large class of threats.

The improvement of training techniques is, therefore, expected to increase the users' security awareness and the efficacy of the already adopted security techniques. The spread of disinformation among less educated people in a time of stressful events has worsened the lack of trust in institutions, leading to violent events and non-compliance with health standards, and left users more vulnerable to social engineering attacks, such as persuasion and fraud. Finally, the expansion of machine learning and AI-based techniques in security has shown their effectiveness in many fields. Their application, as a means to defend users from automated attacks, is increasingly necessary, as the malicious users evolve their methods and adopt AI-based techniques in their attacks.

### 3.2.7. Cross-Cutting Countermeasures and Research Actions

Based on the discussion of respective countermeasures identified regarding multiple domains of interest, these are briefly evaluated and complemented with a description of research actions foreseen.

#### 3.2.7.1. Countermeasures

The following is the list of the countermeasures that apply to more than one domain. More details about the identified countermeasures can be found in the domain-specific countermeasures sections.

**Security by default.** It refers to the technologies which enable security best practices by default, requiring little to no manual intervention. All personnel involved in the design and development of IoT devices should pay attention to security fundamentals and collaborate to accomplish security-by-design. Moreover, network assets and functions should be securely configured according to state-of-the-art practices, while systems should be designed in a way to provide minimum security requirements by deploying a minimum set of security controls. Applications should deploy security by default techniques at all levels, including safe and secure programming language compilers, modern web frameworks, and orchestration platforms that provide automatic encryption and mutual authentication.

**Domains:** IoT/Device, Network, System, Application.

**Firewalls.** Besides being the first line of defense in networks, firewalls can also be used in VMs for monitoring and sifting malicious from good traffic. They can be used to detect various security risks, including phishing attacks, information leaks, incorrect network configurations, malicious code execution, and propagation.

**Domains:** System, User.

**Authentication and Authorization.** It refers to the activities where the user who wants to access a resource is first identified and then authorized. Advance authentication techniques, such as biometrics, multi-factor authentication, and digital certificates can ensure the protection of both IoT endpoints and applications. Combined with authorization, authentication can be successfully used in mitigating security threats.

**Domains:** IoT/Device, Application.

**Enforcing regulations.** More regulations are necessary for ensuring that manufacturers and vendors prioritize security and provide guidelines on the use of the cloud and IoT developers' expectations, thus providing the necessary level of transparency to the organizations and end-users. In addition, some of the already existing policies, such as GDPR and STAR should be applied on the global level.

**Domains:** IoT/Device, System.

**Data encryption.** Encryption is a crucial technique for preserving the confidentiality of the information and fulfilling security strategies and compliance standards. Organizations should define policies of the use of encryption and controls of cryptographic authentication and integrity, including digital signatures and key management. Encryption in virtualized environments is accomplished throughout three distinct phases, namely encryption at data-at-rest, encryption at data-at-transit, and encryption on backup data, while VPNs, HTTPS, SOCKS5, PGP are commonly used for private network communications.

**Domains:** System, Data, User.

**Deploying AI and ML.** AI-based Intrusion Detection Systems (IDS) can be used for monitoring the network, collecting and analyzing information from previous attacks, and ultimately predicting and mitigating incoming attacks. Moreover, real-time ML algorithms, including LDA, random forest, and CART, just to name a few, can be used to identify never-before-seen attacks. Apart from that ML/AI can also be used for processing vast amounts of data across multiple clients and tickets in real-time, correlating those, providing granular attribution and automation actions such as auto-notify and auto-defend actions. This way security awareness training programs can be complemented by assisting in the identification of phishing and spam emails.

**Domains:** IoT/Device, Network.

**Raising security awareness.** Raising security awareness among organizations and end-users is of crucial importance for ensuring the further growth of IoT frameworks and virtualization platforms. Not following the security rules can lead to serious data breaches, which can, in turn, lead to dire consequences. Moreover, an ever-increasing amount of deep fakes, propaganda, misinformation, and disinformation campaigns can affect peoples' everyday life. Hence, gaining knowledge through security awareness campaigns and training sessions is essential for both the end-users and organizations.

**Domains:** IoT/Device, Network, System, Data, User.

**Enforcing access control mechanisms (ACMs).** Access control management (ACM) mechanisms for users, applications, and systems are essential for mitigating the issue of authorization abuse, as well as granting the integrity and confidentiality of resources. They operate per the predefined policies and restrict or limit the capabilities of users to access certain processes. Some of the existing ACM solutions include MAC, RBAC, and CP-ABE.

**Domains:** System, User.

**Security monitoring.** Monitoring network traffic and devices can be a successful way of tracking suspicious activities and performing risk assessments. Captured data can be used for identifying patterns and correlations, inferencing the communication actors and the software used, etc. Based on the results of the analyzed data, further actions such as IoT device revocation and isolation can be enforced. Some tools that can be used for network monitoring include GTP Inspection and GTP Firewall.

**Domains:** IoT/Device, Network, User.

**Firmware maintenance.** Regular firmware updates, monitoring, and maintenance are essential for protecting IoT devices and networks. Additionally, firmware updates should be automatic to ensure secure data transmissions, authorization, and digitally signed network packages. In IoT devices, the secure boot has to be utilized to ensure that a device can only execute OEM or trusted code, thus preventing possible firmware attacks.

**Domains:** IoT/Device, Network.

### 3.2.7.2. Research Actions

The following is the list of the research actions that apply to more than one domain. More details about the identified research actions can be found in the domain-specific research actions sections.

**ML/AI.** Machine learning and AI-based techniques have been used extensively in the prevention and detection of cybersecurity threats in all domains. ML and DL have the potential of leveraging privacy and access control issues, and reinforcing capabilities of attack detection, intrusion detection, malicious code identification, and malware analysis capabilities in IoT environments. However, they come with a significant number of issues that require further research, including the choice of the most suitable model, by-product by-product anomalies that affect critical infrastructure, and real-time applications, as well as legislative issues concerning validation and certification of different IoT components. In the network domain, ML can be utilized for autonomous detection and patching of vulnerabilities to eliminate network threats. However, more research is required in the topics of performing vulnerability assessment and management prioritization and finding efficient techniques for increasing detection accuracy for certain attack types against the overall detection accuracy of the used model. Even though there have already been some efforts of integrating ML and AI capabilities within clouds by tech giants such as Google and Microsoft, ML and AI techniques have to be further integrated to fully harness their potential of reinforcing the security and reliability of cloud solutions and preventing data breaches. In the data domain, the main research challenges include adaptability and introduction of complete automation without, i.e., removal of all human intervention. In the application domain, AI can aid in code analysis, continuous authentication, application, and user monitoring, just to name a few. However, related challenges, limitations, and ways that AI solutions can cause potential voluntary or involuntary damage still have to be better understood. Finally, ML techniques can be utilized for analyzing user interactions, as well as for deploying user identification through biological features, automatic source code, software analysis, as well as security automation. Further research in this field is becoming increasingly necessary due to the growing number of ML-based attacks.

**Domains:** Device/IoT, Network, System, Data, Application, User.

**Blockchain.** At present, IoT devices experience a non-uniform and inconsistent data flow due to conflicting protocols and not standardized designs. Furthermore, most of the vendors do not follow any configuration standards, while IoT infrastructure is mostly centralized, making it susceptible to attacks. Similarly, storing data in centralized structures render it vulnerable to data breaches. Thus, there is a need to conduct more research on adopting decentralized solutions, such as blockchain technology. The benefits of blockchain technology include immutability, verifiability, and efficiency. The combination of blockchain and big data can ensure the trustworthiness and integrity of generated data, as well as keep an immutable record of IoT devices.

**Domains:** Device/IoT, Data.

**Novel authentication schemes.** It refers to novel forms of sophisticated authentication. The effectiveness of the existing protocols and schemes should be further analyzed against malicious activities and especially omnipresent DoS attacks. Future authentication schemes and protocols should be designed with low communication overhead and computation costs in mind. Moreover, future research should focus on the integration and the applicability of passwordless authentication in a larger number and more complex architectures. In the case of IoT environments, novel authentication schemes should be able to cater to all three layers

of IoT architecture and should be operable with an increasing number of nodes without the need to be modified.

**Domains:** Device/IoT, Application.

## 4. Legal Perspectives

In line with the approach taken under D4.2, this Chapter does primarily three things. Firstly, it produces a selective overview of the most relevant regulatory developments that occurred as of December 2020 until the moment of the drafting of this deliverable. Secondly, based on a series of follow-up interviews that were conducted over the last year with cybersecurity stakeholders beyond CONCORDIA consortium, it sheds light on how cybersecurity is implemented in practice, – in the midst, as well, of the COVID-19 pandemic and witnessing how it affects the European Digital Sovereignty - surfacing relevant recommendations. Thirdly, it introduces the Code of Engagement for Threat Intelligence Sharing the current version of which is incorporated under the Appendix B.

### 4.1. Update on the Existing Regulatory Landscape

This section provides an overview of the most relevant regulatory developments concerning the EU Regulatory Landscape that have occurred since the aforementioned submission of the 2<sup>nd</sup> Year Threat Analysis Report. Although the selected legislations are relevant to cybersecurity, the discussion below does not provide exhaustively for all EU regulations pertinent to cybersecurity. The most relevant updates discussed below in alphabetical order relate, mostly to a) the revised Directive on Security of Network and Information Systems (NIS 2 Directive), b) the proposal for the Digital Services Act<sup>98</sup> and the Digital Market Act<sup>99</sup> and c) the Staff Working Report on the impact regarding Cybersecurity of 5G networks<sup>100</sup>.

In the light of the above and drawing upon the domains of the working groups identified under Task 4.1, the table below illustrates the series of already applicable and proposed regulations by Year 3 of CONCORDIA attempting to map them with the focus areas identified, meaning, networks, systems, data, applications and protection of, mostly, the end-user. To this end, the specific mapping was based on the articles providing for the subject matter and the scope under the respective regulation discussed. It should be made explicit that the focus area “people” identified does not only cover end-users, but also people, in general, acting in their other capacities (e.g., employees).<sup>101</sup>

<sup>98</sup> Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, available at: <https://eurlex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN>

<sup>99</sup> Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), available at: <https://eurlex.europa.eu/legalcontent/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN>

<sup>100</sup> ENISA Threat Landscape for 5G networks, available at: [https://www.enisa.europa.eu/publications/enisathreat-landscape-for-5g-networks/at\\_download/fullReport](https://www.enisa.europa.eu/publications/enisathreat-landscape-for-5g-networks/at_download/fullReport)

<sup>101</sup>A former version of this table was included under D4.2, section 4.1.

Table 1: EU legislation and technology domain of interest<sup>102</sup>

Cyber security competence for Research and Innovation					
Selected Applicable / Proposed Legislation	Network	Systems	Data	Application	People
Revised Directive on Security of Network and Information Systems (NIS 2.0)	✓	✓	✓ Data sharing	Impact based?	
Digital Operational Resiliency Act(DORA)	✓	✓	✓	Impact based?	
Cybersecurity Act (CSA)	✓	✓	✓	✓	?
General Data Protection (GDPR)	✓	✓	✓	✓	✓
Free Flow of Non-personal Data (FFDR)		✓	✓	✓	✓
Product Liability Directive (PLD)					✓
Radio Equipment Directive (including Connected Consumer Products)	✓	✓	✓	✓	
Artificial Intelligence Act (AI Act)		✓	✓	✓	✓
Data Governance Act (DGA)		✓	✓	✓	✓
Digital Services Act (DSA)		✓	✓	✓	✓
Resilience of Critical Entities(CER)	✓	✓	✓	✓	✓

Arthur's Legal B.V. 

Note that, as mentioned earlier, in consideration of the EU digital agenda<sup>103</sup>, in addition to the proposed legislative acts captured under the table above, the European Commission has, also, taken a series of new initiatives as, for example, publishing guidelines and conducting public consultations on multifarious topics including cybersecurity. These initiatives have been presented in the EU Cybersecurity Strategy, in Section 1.1 of this document.

#### 4.1.1. The Directive on Security of Network and Information Systems (NIS Directive)

Aiming to update the existing legal cybersecurity framework to reflect the ongoing digital transformation of society, the European Commission proposed the NIS2 Directive to update its 2016 predecessor. On 28 October 2021, the European Parliament's Committee on Industry, Research and Energy (ITRE) adopted the NIS2 Directive proposed by the European Commission. The Parliament is expected to vote on the text in its plenary on 10 November 2021. Getting the NIS2 Directive into force will repeal the current NIS Directive from 2016 (2016/1148)<sup>104</sup>. The draft proposal of the NIS2 Directive has been described and assessed in Deliverable D4.2 already. Hence, the paragraph of this deliverable (D4.3) merely summarizes the current state of play of the adopted NIS2 Directive:

The ongoing transformation in this Digital Age has expanded the threat landscape and presented new cybersecurity challenges that require adapted and innovative responses.

<sup>102</sup> Although of interest for CONCORDIA, the eIDAS Regulation has not been specifically included in this Deliverable and in the Table 1. In this regard, we refer to what has been discussed in Deliverable D4.2, Section 4.2.7.

<sup>103</sup> European Commission, Europe's Digital Decade: digital targets for 2030 (Brussels, 09/032021). [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en)

<sup>104</sup> Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

The new mission is to improve European cyber resilience by addressing the deficiencies of the 2019 NIS Directive, mainly by expanding the scope, including new or updated (i) obligations to adopt national cybersecurity strategies, and to designate competent national authorities/single points of contact/CSIRTs, (ii) cybersecurity risk management and reporting obligations for ‘essential entities’ and (iii) obligations on cybersecurity information sharing.

The NIS2 Directive is built on three (3) main pillars, it focuses on improving Member State cybersecurity capabilities, developing cybersecurity risk management in the internal market and encouraging information sharing.

One of the main changes under the NIS2 is the expansion of the application of cybersecurity to new sectors, in addition to introducing quantifications thresholds to underline the inclusion of medium-sized and large companies. The involvement of smaller actors is left to the discretion of Member States to decide on whether or not they belong to critical infrastructure. The NIS2 Directive is to form one of the baselines for the European cybersecurity framework and to be a central tool in advancing Europe’s digital sovereignty-related programs of the Commission.

To conclude this brief overview, four notable key elements in the NIS2 Directive are:

1. The elimination of the distinction between operators of essential services and digital service providers, identifying certain ‘essential’ sectors (energy, transport, FSI, health, water, digital infrastructures, public administration and space);
2. Strengthening of the security requirements for companies by imposing a risk management approach providing a list of basic security elements that have to be applied;
3. The introduction of more precise provisions regarding the process for incident reporting, the content of the reports and timelines;
4. The imposition of obligations requiring companies to address cybersecurity risks in supply chains and supplier relationships. Member States and ENISA will carry out a coordinated risk assessment of critical supply chains building on the approach taken in the context of the recommendations on cybersecurity of 5G networks.

It must be signaled that at the moment of the drafting of the present deliverable, the developments pertinent to the NIS2 Directive are already progressing. They will be further monitored and documented as appropriate under forthcoming CONCORDIA deliverables and, mainly, under CONCORDIA Roadmap, due at the end of the project.

#### **4.1.2. The Regulation on ENISA and on Information and Communications Technology Cybersecurity Certification (Cybersecurity Act)**

As discussed under the aforementioned D4.2 submitted in December 2020, the Regulation on the European Union Agency for Cybersecurity (ENISA) and on information and communications technology cybersecurity certification<sup>105</sup> (CSA) had the dual objective to

---

<sup>105</sup> Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

strengthen ENISA and to create an EU-wide cybersecurity certification framework for digital products, services and processes.

In line with these objectives, and in accordance with the duty assigned to ENISA under Article 7 of the CSA regarding situational awareness, the agency has issued a series of reports, including the ENISA Threat Landscape 2021 report. As explicitly mentioned in the latter, findings such as the creation of a timeline of observed incidents related to major ETL threats (OSINT-based situational awareness) in terms of their proximity or the identification of the targeted sectors per number of incidents (April 2020-July 2021) fall under ENISA's task in relation to situational awareness. As far as the creation of the earlier stated EU-wide cybersecurity certification framework is concerned, over the last year, several developments took place, including the release of the draft version of the EUCS candidate scheme (European Cybersecurity Certification Scheme for Cloud Services),<sup>106</sup> which looks into the certification of the cybersecurity of cloud services and which serves as a basis for external review.

Note that, same as it is the case for all EU legislative acts that have the form of a regulation and they are, thus, directly applicable with direct effects across the EU, Member States must publish a reception act for the CSA to become integral part of the respective national legal orders.

#### 4.1.3. General Data Protection Regulation (GDPR)

The main developments pertinent to the GDPR<sup>107</sup>, that took place as of the time of the submission of D4.2 in December 2020 up to the moment of the drafting of the present deliverable, relate to a) the publication of the Commission's Decisions on Standard Contractual Clauses between Controllers and Processors<sup>108</sup>, b) on Transfers of Personal Data to Third Countries<sup>109</sup>, and c) to the publication of an Adequacy Decision allowing for the Transfer of Personal Data to the UK<sup>110</sup>.

---

OJ L 151 <sup>182</sup> ENISA, COVID-19 webpage, available at: <https://www.enisa.europa.eu/topics/wfh-COVID-19?tab=details>

<sup>106</sup> EUCS, a candidate cybersecurity certification scheme for cloud services, available at: <https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme>

<sup>107</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119

<sup>108</sup> Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0915&locale=en>

<sup>109</sup> Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at: [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en)

<sup>110</sup> European Commission, 'Data protection: Commission adopts adequacy decisions for the UK' (Brussels, 28 June 2021). European Commission, 'Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade' (Brussels, 16 December 2020) 18 final. <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>

Furthermore, in the course of 2021 and despite the impact of the COVID-19 pandemic in the public sector, both the European Data Protection Board (EDPB), as well as the national Data Protection Authorities have been quite active by taking several enforcement actions.

#### 4.1.4. The Regulation on the Free Flow of Non-Personal Data

Given that the relevant regulation<sup>111</sup> provided that the Member States had time until 30 May 2021 to repeal any existing data localization requirement that is laid down in law, regulation, or administrative provision of a general nature, it is expected that at the moment of writing this deliverable, Member States must have complied with this obligation. However, there is currently no publicly available information producing an overview in this respect at the level of the EU.

As far as the various switching Codes of Conduct being developed under the above-mentioned Regulation in light of Article 6 on porting of data, the SWIPO (Switching and Porting) Codes of Conduct have been presented by the SWIPO Working Group to the European Council and the EU Commission and it is intended that they are evaluated by the European Commission before November 2022. Note that the Codes of Conduct themselves, including of course, the related documentation for adherence (e.g. adherence declaration form) are publicly available<sup>112</sup>.

#### 4.1.5. Product Liability Directive (Liability for AI-enabled Products and Services)

On 20 October 2021, the Commission has launched a public consultation on the rules on compensation for damage caused by defective products.<sup>113</sup> A specific focus is on the use of Artificial Intelligence (AI) in products and services. The consultation asks whether the rules set out in the Product Liability Directive, together with other national liability rules, still provide legal certainty and consumer protection in the age of smart and AI-based products and services. Building on the “2018 Evaluation of the PLD”,<sup>114</sup> which identified several shortcomings in relation to digital technologies in general, the Commission points out three problematic issues.

The first concerns the intangibility of digital products. Digital content, software and data play a crucial role in the safe functioning of many products, but it is not clear to what extent such intangible elements can be classified as products under the Directive. It is therefore unclear whether injured parties will always be compensated for damage caused by software, including updates, and who will be liable for such damage. The second concerns connectivity and cybersecurity. New technologies bring with them new risks, such as openness to data inputs that affect safety, cybersecurity risks, risks of damage to digital assets or privacy

---

<sup>111</sup> Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union OJ L 303

<sup>112</sup> For more information, see, also, <https://swipo.eu/code-adherence/>

<sup>113</sup> The consultation is open for 12 weeks and will run until 10 January. See here an overview of the consultation: [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en)

<sup>114</sup> European Commission, REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC) (Brussels, 7 May 2018) <https://ec.europa.eu/docsroom/documents/29233>

infringements. The Directive provides only for compensation for physical or material damage and it is unclear if the definition of a defect covers cyber vulnerabilities.

The third concerns complexity of digital technologies. For instance, regarding IoT systems, it is challenging for the injured party to identify the responsible producer. According to the Commission, these challenges and uncertainties have negative consequences for both businesses and consumers. If companies face legal uncertainty due to outdated and unclear EU and (divergent) national liability rules, this could leave producers, service providers and operators unable to assess the extent of their liability. This could create extra costs, stifle innovation and discourage investment. Injured parties could experience difficulties getting compensation for harm caused by digital technologies. If consumers had less protection compared to those who suffered damage caused by traditional technologies, this could undermine societal trust in and uptake of emerging technologies.

#### 4.1.6. Radio Equipment Directive

The Directive on the harmonization of the laws of the Member States relating to the availability of radio equipment<sup>115</sup> (RED) on the market, provides a framework for that very objective. As discussed in D4.1, the RED applies to electrical or electronic products, which intentionally emit and/or receive radio waves for the purpose of radio communication and/or radio determination, or electrical or electronic products which must be completed with an accessory, such as an antenna, to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radio determination.<sup>116</sup> The RED provides a framework to ensure that such products meet certain standards for various aspects including safety, health and electromagnetic compatibility.

On 29 October 2021, the Commission adopted a Delegated Act of the Radio Equipment Directive (hereto, Delegated Act) activating Articles 3(3)(d), (e) and (f) for certain categories of radio equipment to increase the level of cybersecurity, personal data protection and privacy.

As mobile phones, smartwatches, fitness trackers and wireless toys are more and more present in our everyday life, cyber threats pose a growing risk for every consumer. The adopted Delegated Act aims to ensure that all wireless devices are safe before being sold on the EU market. This Act lays down new legal requirements for cybersecurity safeguards, which manufacturers will have to take into account in the design and production of the concerned products. It will also protect citizens' privacy and personal data, prevent the risks of monetary fraud as well as ensure better resilience of our communication networks.

According to Thierry Breton, Commissioner for the Internal Market, the requirements envisaged in the Delegated Act will greatly improve the security of a broad range of products,

---

<sup>115</sup> Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC OJ L 153

<sup>116</sup> Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC OJ L 153 Article 2(1)(1).

establishing a comprehensive set of common European Cybersecurity standards for the products (including connected objects) and services brought to the EU market.

The measures proposed cover wireless devices such as mobile phones, tablets and other products capable of communicating over the internet; toys and childcare equipment such as baby monitors; as well as a range of wearable equipment such as smartwatches or fitness trackers. The Delegated Act will be complemented by a Cyber Resilience Act. The Delegated Act will come into force following a two-month scrutiny period, should the Council and Parliament not raise any objections.

Following the entry into force, manufacturers will have a transition period of 30 months to start complying with the new legal requirements. This will provide the industry with sufficient time to adapt relevant products before the new requirements become applicable, expected as of mid-2024.

The Commission will also support the manufacturers to comply with the new requirements by asking the European Standardization Organizations to develop relevant standards. Alternatively, manufacturers will also be able to prove the conformity of their products by ensuring their assessment by relevant notified bodies.

#### **4.1.7. Regulation for European Cybersecurity Competence Centre**

In May 2021, the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (ECCC) was approved.<sup>117</sup> As mentioned in the Deliverable D4.2, this regulation is especially of relevance to CONCORDIA, given the similarities in objectives between the latter and the ECCC.

ECCC improves coordination on cybersecurity across Europe. Using the words of its Interim-Director, Miguel Gonzalez Sancho, ECCC's goal is to build proactive capacity in the field of cybersecurity, which is a strategic priority for the EU. Specifically, ECCC's effort is concentrated on three areas: (i) managing EU funding requirements for capacity building; (ii) coordination of national Competence centres; (iii) building the European cybersecurity community, starting from the four pilots (CONCORDIA being one).

In this sense, the ECCC is part of a bigger effort, which in the last year has seen the Commission and other EU institutions committed to proposing new regulations and investments. In this bigger picture, the ECCC will coordinate funding from the EU to national cybersecurity centres.<sup>118</sup> For this purpose, EU Commission has issued guidelines on the assessment of the capacity of National Coordination Centres to manage funds to fulfil the mission and objectives laid down in Regulation (EU) 2021/887. Additional to EU funds, MS and the private sector should contribute to the effort.

---

<sup>117</sup> REGULATION (EU) 2021/887 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

<sup>118</sup> European Commission, COMMUNICATION FROM THE COMMISSION Guidelines on the assessment of the capacity of National Coordination Centres to manage funds to fulfil the mission and objectives laid down in Regulation (EU) 2021/887. <https://digital-strategy.ec.europa.eu/en/library/guidelines-assessment-capacity-national-coordination-centres-manage-funds-fulfil-mission-and>

The ECCC is in the process of selecting a new director. A strategic advisory group will be selected as well. The selection is carried out in a transparent manner, which keeps into account representation of different backgrounds and competences. For this selection, no timetable is still available. In early 2022, the ECCC will issue calls for proposal through the Digital Europe fund.

## **4.2. Update on the Upcoming Regulatory Landscape**

This section provides an overview of the most relevant, possibly upcoming, EU legislative initiatives related to the project's scope. Note that, at the moment of the drafting of the present document, these legislative initiatives are at a proposal stage, thus they are not binding. Nevertheless, even though their adoption is not certain, as they are subject to further discussions between the European Parliament and the Council of the European Union, they provide valuable insights on the objectives of the European Digital Agenda (listed below in alphabetical order).

### **4.2.1. Artificial Intelligence Act (AI Act)**

On 21 April 2021, the European Commission presented the Artificial Intelligence Act (AI Act) proposal.<sup>119</sup> The proposal sets out horizontal rules for the development, commodification and use of AI-driven products, services, and systems within the territory of the EU. The draft regulation provides core artificial intelligence rules that apply to all industries. The AI Act introduces a sophisticated 'product safety framework' constructed around a set of four risk categories. It imposes requirements for market entrance and certification of High-Risk AI Systems through a mandatory CE-marking procedure. To ensure equitable outcomes, this pre-market conformity regime also applies to machine learning training, testing and validation datasets. The proposed AI Act seeks to codify the high standards of the EU trustworthy AI paradigm, which requires AI to be legally, ethically and technically robust, while respecting democratic values, human rights and the rule of law.

The Artificial Intelligence Act proposal combines a risk-based approach based on the pyramid of criticality, with a modern, layered enforcement mechanism. This means, among other things, that a lighter legal regime applies to AI applications with negligible risk, and that applications with an unacceptable risk are banned. Between these extremes of the spectrum, stricter regulations apply as risk increases. These range from non-binding self-regulatory soft law impact assessments accompanied by codes of conduct to heavy, externally audited compliance requirements throughout the life cycle of the application.

The proposal provides for the installation of a new enforcement body at the level of the Union: The European Artificial Intelligence Board (EAIB). At the level of Member States, the EAIB will be flanked by national supervisors, similar to the GDPR's oversight mechanism. Fines for violation of the rules can be up to 6% of global turnover, or 30 million € for private entities.<sup>120</sup>

---

<sup>119</sup> European Commission, 'Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts' COM(2021) 206 final (Brussels, 21.4.2021).

<sup>120</sup> Mauritz Kop, 'EU Artificial Intelligence Act: The European Approach to AI (Stanford Law, 1/10/2021) <https://law.stanford.edu/publications/eu-artificial-intelligence-act-the-european-approach-to-ai/>

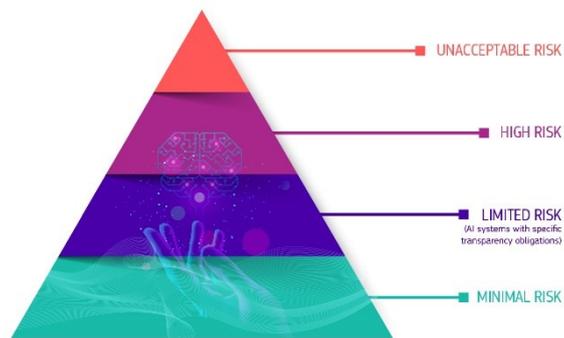


Figure 3: Pyramid of Risk

#### 4.2.2. The Data Governance Act (DGA)

On 25<sup>th</sup> November 2020, European Commission published a Proposal for a Regulation on European data governance (Data Governance Act)<sup>121</sup>. On 24 September 2021, the Council adopted its position, and the proposal is now under negotiation in ‘trilogues’.<sup>122</sup>

The overarching objective of the proposal is to strengthen the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU. Specifically, the proposed act:

(i) introduces conditions under which public sector bodies may allow the re-use of certain data they hold, notably data, which is protected on the grounds of commercial confidentiality, statistical confidentiality, protection of intellectual property rights of third parties or the protection of personal data. The proposed regulation, therefore, complements the Open Data Directive by addressing data that cannot be made available as open data. Public sector bodies allowing re-use must safeguard the protection of rights and interests of third parties, for instance, through technical means, such as anonymization or secure processing environments, or by supporting the satisfaction of legal basis, for instance by supporting potential reuse in seeking consent from the data subjects.

(ii) imposes obligations on providers facilitating the sharing of personal and non-personal data. In particular, service providers shall remain neutral as regards the data exchanged between data holders and data users. They should only act as intermediaries in the transactions and may not use the data exchanged for any other purpose. To avoid a conflict of interests, additional services would need to be structurally separated and provided for through a separate legal entity. A competent authority designated by the Member States would monitor compliance and be able to impose fines and periodic penalty payments as well as require the cessation or postponement of the service in case of a breach.

<sup>121</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act), Brussels, 25.11.2020 COM (2020) 767 final 2020/0340 (COD). For more information, see also <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act>

<sup>122</sup> Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) - Mandate for negotiations with the European Parliament (Brussels, 24 September 2021).

(iii) establishes a ‘register of recognized data altruism organizations’ in order to increase trust in the operations of registered organizations that facilitate the voluntary sharing of data for the common good. An entity that does not meet certain transparency requirements or insufficiently safeguards the rights of data subjects and legal entities, may be removed from the register. The Commission announced it would develop a common European data altruism consent form to lower the costs of collecting consent and to facilitate data portability.

(iv) creates a formal expert group, namely the ‘European Data Innovation Board’. The board is tasked with facilitating the emergence of best practices and the consistent application of the framework, as well as with advising on the governance of cross-sectoral standardization. The board would be composed of representatives of Member States’ authorities, the European Data Protection Board, the Commission and various other representatives.

Based on that current draft, several observations can be made. The draft DGA pays due attention to key concepts, such as trust and trust components in security, cybersecurity and (data) protection. In this sense, and in consistency with other relevant legislations, such as the GDPR and FFDR, the draft DGA presents itself as a horizontal, risk-based and data-centric but also mission-driven regulation. This is also visible in consideration of the keywords used often in the draft DGA, for instance: ‘secure’ (16 times, including referring to secure processing), ‘security’ (18 times, including referring to national security), and ‘protection’ (72 times, obviously including but not only: data protection). Moreover, similarities with the GDPR are noteworthy. Both the clause regarding transparency requirements (Article 18) and the specific requirements to safeguard rights and interests of data subjects and data holders as regards to their data (Article 19), can be traced back to what is envisaged in the GDPR. Nevertheless, the recently approved Council’s text includes a clearer delineation for situations when personal data are concerned and makes it explicit that the DGA does not create a legal basis for personal data processing.<sup>123</sup>

The draft DGA explicitly mentions the requirement to meet the appropriate level of security for the storage and transmission of non-personal data. (This requirement is well-known in the cybersecurity community, as per Clauses 25 and 32 of GDPR, which address the requirement for the continuous appropriate dynamic accountability, respectively from data processing and data protection perspectives.) The principle-based and contextual approach of what is appropriate and what is not, will for sure be a quite relevant topic and dimension for the cybersecurity community – both in the private sector as well as the public sector – including the relevant authorities and agencies – to implement, cater for, configuration and continuously monitor and optimize.

There are connections beyond the GDPR. For instance, the draft DGA explicitly mentions strategic data and sensitive data. In this sense, the draft is inspired by, or even links to, the current structure of the obligation to inform, as well as other data sharing obligations, which are envisaged in the NIS Directive. These ISAC schemes are generally well known from the cybersecurity community, both in the public sector and private sector (especially in the context of critical infrastructure, vital systems or essential services domains).

---

<sup>123</sup>Council of the European Union, *supra*.

### 4.2.3. Digital Operational Resilience Act

On 24 September 2020, the European Commission published its draft Digital Operational Resilience Act (DORA).<sup>124</sup> The legislative proposal builds on existing information and communications technology (ICT) risk management requirements already developed by other EU institutions and ties together several recent EU initiatives into one Regulation. In this regard, DORA is *lex specialis* in respect of NIS.

DORA aims to establish a much clearer foundation for EU financial regulators and supervisors to be able to expand their focus from ensuring firms remain financially resilient to also making sure they can maintain resilient operations through a severe operational disruption.

### 4.2.4. Digital Services Act (DSA) and Digital Markets Act (DMA)

On 16 December 2020, both the proposal for the Digital Services Act (DSA),<sup>125</sup> as well as the proposal for the Digital Markets Act (DMA) were published.<sup>126</sup>

Regarding these two policy initiatives, Unit F2 (E-Commerce & Platforms) of DG Connect's Directorate F (Digital Single Market) is leading, where DG Competition is closely involved in the latter one (DMA) as well. Hereunder both DSA and DMA are discussed, mainly from the perspectives of transparency, trust, accountability, and other digital sovereignty perspectives, which are all components directly related to (cyber)security and the mission of CONCORDIA, the Commission and its many other stakeholders.

The DSA will replace the (outdated) 2000 e-Commerce Directive.<sup>127</sup> The DSA will apply to providers of digital intermediary services, which includes mere conduit, caching or hosting services. The DSA has an extraterritorial effect, and for once determines a liability regime and additional obligations related to the spreading of hate speech, misinformation and other illegal content, including how to respond.

The DSA provides for a new transparency and accountability framework regarding societal responsibilities with the aim of catering for building, achieving and sustaining digital sovereignty, including such for individuals and organizations within the EU. With the DSA, for instance, tools to hold platforms accountable for algorithm transparency, data usage and

---

<sup>124</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 COM/2020/595 final, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595>

<sup>125</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final, available at: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN>

<sup>126</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act). COM/2020/842 final, available at: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN>

risk-mitigation are introduced, by means of (A) additional systemic risk management requirements for large online platforms with more than 45 million users – (which method is one of the key parameters within the DSA), (B) additional transparency requirements for online advertising toward individual recipients (including the obligation to provide for details about the advertising buyer and parameters used to determine the recipient to whom the ad is displayed), and the requirement of the large online platforms to appoint qualified compliance officers.

Keywords related to digital sovereignty and strategic autonomy that are therefore used often in the DSA are notably transparency, fairness, accountability, protection (including protection of fundamental rights and freedoms, and consumer protection), safety and secure data storage. In short, a framework that tries to strike the balance between the plethora of (and in many cases on contextual level clashing) fundamental rights and freedoms as well as responsibilities of online platforms on which so many depend nowadays.

Regarding the Proposal for Digital Markets Act (DMA), the competition law component – another digital sovereignty component, as also highlighted and addressed in the Cybersecurity Roadmap for Europe by CONCORDIA (M24 and M36) - was already pre-announced in the European Commission's data strategy.

The DMA is built around the notion of gatekeepers, being companies that (A) provide certain core platform services in at least three (3) member states, (B) meet certain thresholds of (B1) EEA turnover or market capitalization and fair market value, as well as (B2) have a minimum number of active end/business users in the EEA in the last three financial years. Same as the DSA, the DMA has an extraterritorial effect. Examples of core platform services are (for instance) online intermediation services, search engines, social networking services, video-sharing platforms and cloud computing services.

Gatekeepers under the DMA are subject to an extensive list of do's and don'ts, with potential hefty fines and other remedies available to regulators. The DMA also foresees the creation of a Digital Markets Advisory Committee. In short, the DMA is also doing its part in facilitating the (re)building, achieving and sustaining of digital sovereignty.

#### **4.2.5. Resilience of Critical Entities Act (CER)**

On 16 December 2020, the EU Commission presented a proposal for a directive on the resilience of critical entities.<sup>128</sup> This proposal is closely aligned and establishes close synergies with the at the time proposed NIS 2 Directive, which aims at enhancing all-hazards information and communication technology (ICT) resilience on the part of 'essential entities' and 'important entities' meeting specific thresholds in a large number of sectors. With this proposal, the Commission intends to create an all-hazards framework to support the Member States in ensuring that critical entities are able to prevent, resist, absorb and recover from disruptive incidents, no matter if they are caused by natural hazards, accidents, terrorism, insider threats, or public health emergencies like the one the world faces today. The

---

<sup>128</sup> Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities COM/2020/829 final, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN>

proposal, which covers ten sectors, namely energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space.

The proposal includes some noteworthy provisions, listed below in no particular order. The Member States would be obligated, among other things, to have a strategy for ensuring the resilience of critical entities, carry out a national risk assessment and, on this basis, identify critical entities. Critical entities would be required to carry out risk assessments of their own, take appropriate technical and organizational measures in order to boost resilience, and report disruptive incidents to national authorities. Critical entities providing services to or in at least one-third of Member States would be subject to specific oversight, including advisory missions organized by the Commission. The Commission would offer different forms of support to the Member States and critical entities, a Union-level risk overview, best practices, methodologies, cross-border training activities and exercises to test the resilience of critical entities. Regular cross-border cooperation with regard to the implementation of the directive would be facilitated through an expert group, the Critical Entities Resilience Group.

This proposal also aims to ensure that competent authorities designated under this directive and those designated under the proposed NIS 2 Directive take complementary measures and exchange information as necessary regarding cyber and non-cyber resilience, and these particularly critical entities in the sectors considered to be ‘essential’ per the proposed NIS 2 Directive, are also subject to more general resilience-enhancing obligations to address non-cyber risks.

#### **4.2.6. Other Legislative Initiatives**

This section presents the legislative initiatives, which has neither been formalized in a proposal yet nor represents updates to existing legislations.

##### **Data Act**

In its Data Strategy of February 2019, the Commission has formulated a vision to support data-driven innovation, increase the availability of data in a secure and otherwise trusted way, enable the usability of data to support sustainable growth and innovation across all sectors, helping develop evidence-based policies and services as well as to contribute to the European Green Deal.

In May 2021, the Commission published its Inception Impact Assessments on the forthcoming Data Act. The Data Act initiative aims to establish a horizontal framework that would complement the proposed Data Governance Act (DGA). The two initiatives aim to create trust and fairness in the data economy by addressing the difficulties of access to and use of certain data in specific situations, including in a B2B and B2G context. One of the objectives is to give people, society and the private sector more control, conditions and other trust parameters over shared data, information and other attributes. To complement these initiatives, the Commission also aims to revise the Database Directive and to assess the Trade Secrets Directive.

On 27 September 2021, the Regulatory Scrutiny Board (RSB) rejected the draft Data Act, mainly for concerns regarding the conditions for public bodies to access data, the level of sufficient information on the compensation for businesses, and the level of clarity of interplay with other regulation and legislation. These concerns are currently in process of being addressed, with an anticipated delay towards adoption until the first quarter of 2022. Nevertheless, from a security, cybersecurity and (data) protection perspective, currently, the DGA is seen as more relevant for CONCORDIA, the mission of the Commission regarding CONCORDIA and the other pilots, and this deliverable.

### **European Chips Act**

On 15 September 2021, European Commission President Ursula von der Leyen announced the intention to present a European Chips Act. This initiative is meant to boost Europe's semiconductor capacity and reinforce its new drive for strategic autonomy.

According to Commission President, in consideration of the current global demand spike, Europe's share across the entire value chain, from design to manufacturing capacity, has shrunk. This has implications not only on European economic competitiveness, but also increases reliance on state-of-the-art chips manufactured in Asia, which undermines Europe's tech sovereignty. The initiative should focus on three objectives: firstly, a European Semiconductor Research Strategy; secondly, a collective plan to enhance European semiconductors production capacity; thirdly, a framework for international cooperation and partnership.

The initiative does not come without criticism from certain industry stakeholders, which are wary that the chips act will be driven more by political considerations than market needs. A proposal is expected in 2022.

## **4.3. Implementing Cybersecurity Principles: The Interview Series 2020**

This section focuses on the findings of the interviews conducted in 2020 and 2021 with experts within CONCORDIA and beyond.

### **4.3.1. From Why to How**

In the past period, the discussion about the 'why' of cybersecurity and the related non-functionals such as security, data protection, privacy, e-privacy and cyber-physical safety has finally been settled. All stakeholders nowadays agree (to a certain, contextualized extent) that cybersecurity is a need-to-have, and it is high time to focus on, address and implement the 'how'. How to implement cybersecurity, safety and privacy principles in practice, all the way upstream by design as well as further midstream, side stream and all the way downstream? How to do so, while including the organizational, societal, psychological, and economical aspects as well as the preconditions and net-benefits of implementing and keeping up to date and resilient?

Where in 2020 CONCORDIA started its series of qualitative interviews about the 'how' with experts within the CONCORDIA consortium, in 2021 interviews have been conducted with experts, mostly beyond the CONCORDIA consortium, representing NGOs, policy makers, industry and academia both at national, European and international level.

Same as in 2020 the 2021-interviews were set up and done in an open dialogue mode (under Chatham House Rule), without fixed questions. However, each was prepared and calibrated with each interviewee before the dialogue, where at least certain scoping and guidance was provided by means of the methodology of State of the Art (SOTA) minus (-/-) State of Play (SOP) equals GAP, and what are, would or could be GAP recommendations, and which ones are doable, feasible and affordable (or not), and why. This methodology is the same as used during the interview series 2020, where in 2021 the overarching dimension was digital sovereignty (or open strategic autonomy) including without limitation awareness, global internet, security, cybersecurity, safety, (personal) data protection, consumer and other societal protection, competition, accountability, transparency, trust, and trustworthiness. Therefore, the interview series of 2021 used the visualisation outlined in Figure 4, below.

## By Design, Implementation & Societal Aspects of Digital Sovereignty Principles

Input from Experts Beyond the Consortium Consortium



Figure 4: Digital Sovereignty Principles

### 4.3.2. Two Main Common Denominators in the Interview Series 2021

A common denominator that has been perceived during the interviews conducted up to the date of the edition of this deliverable is the global COVID-19 pandemic, and the fact that it has further accelerated the Digital Age. This acceleration has further increased (or otherwise demonstrated) the dependability to digital technology, devices, systems, data flows, services, manufacturers, vendors and suppliers, with substantial and sometimes critical and otherwise vital (positive and negative) impact to people, society, governments, healthcare, supply chains and other sectors.

A conclusion of this common denominator is that it has been proven that digital sovereignty is one of the key necessities of and objectives within the European Union, but it also proves that the level of digital sovereignty (from the perspectives of individuals, organisations, member states, or regions, either Union or global) may have decreased during the – still ongoing – pandemic. Where during the pandemic working online worked better than offline, the working happened on certain platforms, in systems and with services that were not necessarily fully secure, privacy-preserving, transparent, accountable, assured or otherwise under meaningful control and appropriate rule of law.

In brief, a global pandemic is not beneficial for building, achieving or sustaining digital sovereignty in or within the European Union, but it has brought an increased level of

awareness including identifying where digital infrastructures are not sufficiently in place, where member states and other organisations were or are not prepared, demonstrating the vulnerabilities and other weaknesses, as well as showing the benefits of the Digital Age.

On the bright side, this net-negative awareness can now be used as an additional incentive to reverse this movement and put additional focus and put resources in building, achieving and sustaining digital sovereignty. Although not an extensive part of the interviews, both national initiatives as well as European ones such as the Recover and Resilience Facility (RRF) with the current total of EUR723.8B<sup>129</sup>, where in each national recovery and resilience plan a minimum of 20% of expenditure needs to be allotted to foster the digital transition and related reforms and investments. All scenarios should have digital objectives to push the digital economy and society, based on the three main pillars of the European Commission: more green, more digital and more resilience. The RRF is quite aligned with the objectives regarding digital sovereignty. The other, more specific perspectives per interview, outlined in the following paragraphs, are in no particular order.

#### **4.3.3. Implementing Digital Sovereignty Principles: International Privacy Law Perspective**

From the perspective of the General Data Protection Regulation (GDPR), as well as international privacy law, the global COVID-19 pandemic has raised many concerns. For instance, which law is applicable when in a cross-border conference call? The participants are in different jurisdictions, the mobiles or other devices – and their operating systems – are governed by one of several technology companies on the other side of the globe, the Web servers and other hardware may be running somewhere else (and probably in multiple and unknown jurisdictions), while the data may be transmitted over other – national or other – communication networks and infrastructure. Meanwhile, people, the public sector, private sector, academia and society at large are trusting and depending on this complex – and every changing – set of technical stack and technical, organizational and jurisdiction dimensions.

Where the GDPR not only had a positive effect – or at least notable impact – to the appropriate levels of data processing, data protection, security and data management within the digital, cyber-physical and other relevant domains within EU, EEA and its periphery, it has also had a notable impact in other parts of the world. It, however, also leads to confusion, questions and conflicting situations as international privacy law is still quite local, per jurisdiction, and not always aligned or otherwise interoperable with each other. There is quite some overlap, vault lines as well as grey areas. This means that an individual does not know what rights and obligations it has. The same goes for the vendor side, the demand side and for data protection authorities. In general, each stakeholder has taken a too simplistic approach on global, overlapping privacy and personal data protection, also for and the benefit of protecting European citizens, values and interests.

One of the other reasons why these confusion and conflicts are present is that privacy law is – mostly – administrative law. In most jurisdictions it is – still – not a private/civil law, with direct rights, redress and remedies for the individual; a national person. The GDPR is

---

<sup>129</sup> The Recovery and Resilience Facility: [https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility\\_en](https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility_en)

a hybrid law, being both administrative and private/civil law, which from an interoperability point of view brings extra complexity in the international domain.

Furthermore, the imbalance while using digital products, systems and services is not yet catered for, and generally controlled – at the detriment of people and society – by large or otherwise powerful corporations. Where, in the past one had a choice to go online or not, nowadays, it is a necessity to be online, in order to work, communicate, do transactions and otherwise engage. IoT and other cyber-physical systems, connected devices and related services augment the integration between offline and online, and therefore the dependability. Meanwhile, an operating system (OS) is much closer to the individual than the rule of law. If a big tech company changes its terms of service (which it still can, unilaterally), it has a bigger impact than a change of law by the bigger countries, federations or unions in the world. The roles between such tech companies and such countries, federations and unions – including the EU – are still a work in progress, while the territory ahead becomes even more hazardous (including the developments related to AI).

All in all, this does not necessarily cater for more digital sovereignty, and needs more attention and more transparency, to the extent possible, alignment, coordination and orchestration (and, where possible a global treaty) with and by the European Union, its internal stakeholders as well external ones, most notably its allies and friends. This holds especially true, considering that digital sovereignty does not start at the borders of the EU, but that is essentially of interest for the digital domains globally.

Accountability and having a principle-based approach, form the two identified common denominators. The principle-based approach has been deep-dived into in the interview series 2020 (as reported in D4.2). First, accountability is a dimension, agnostic, technology-neutral and can be applied in almost every jurisdiction. It has universal capabilities, where it is also already a cornerstone of the GDPR. So, accountability – and therewith, building trust and providing a tool to demonstrate the appropriate level of data processing, protection, and the like – has been identified as a key component to digital sovereignty.

#### **4.3.4. Implementing Digital Sovereignty Principles: Accountability perspective**

The term digital sovereignty is not always interpreted – or perceived – in the same way. There is a lot of confusion about it, also outside the EU. One the reasons may be that traditionally nations have monopolized the term sovereignty, where nowadays it is also used from individual-level or human rights-perspective (self-sovereignty), data-perspective (data sovereignty), society, organizations, and Union-perspectives. The definition to have the ability and degree to have meaningful control applies to each of these perspectives.

Another angle to focus on, in order to avoid discussion about who has what digital sovereignty where, is accountability. As mentioned before, it is an all-present, agnostic, and versatile term. It provides for a dynamic framework – and validation tool – to do scenarios, keep in check and continuously improve real-life situations.

Without accountability, no trustworthiness can be demonstrated, and no trust can be built. It can be deployed both ‘before, during and after’, meaning in design, development, and pre-deployment/production phases, respectively during deployment, production and use, as well as thereafter. It can address the various technical layers, domains, and related dimensions (such as the human factor, data, identity, authorization, and the like), as it can also

address whole ecosystems. Therefore, the approach of CONCORDIA to have a x-centric approach works nicely with accountability too.

Accountability can furthermore also be deployed from different notions of use, for instance, intended use, expected use and actual use. As accountability works well in combination with stakeholders plotting, any context, risk and impact assessments, scenario plotting as well as with personal, societal and economical and ecological values and interests, it can identify the appropriate level of accountability for each of these uses – which generally differ, as per the nature of the current digital products, systems and services with which businesses, households, society and even countries are run.

#### **4.3.5. Implementing Digital Sovereignty Principles: Policy Making Perspective**

As mentioned above, in the paragraph about the proposals for the Digital Service Act (DSA) respectively the Digital Market Act (DMA), part of policy making is catch up, including revising and other updating outdated directives, such as the e-Commerce Directive (which is already more than 20 years old, and had been outstripped by the many technological and related developments in this Digital Age). Another part is to come with technological-neutral, future-proof additional frameworks that are fit and can cater for the existing and new outcries, excesses, problems and challenges to people, organizations, member states and society at large face nowadays, such as hate speech, unsafe products, disinformation, surveillance-based advertising, illegal content, and the like.

The DSA for sure is a new transparency and accountability framework. The current (draft) proposal is very much built and fit for building, achieving and sustaining digital sovereignty within the EU. However, it is obviously not a single silver bullet, it also as such does not exist in this complex and converging digital world, which is global.

The DSA is system-centric or said otherwise platform-centric or digital ecosystem-centric. This provides for supervision, oversight, and the potential consistency and therewith trust in these systems. Therefore, the approach of CONCORDIA to have an x-centric approach – including a holistic, system-centric, platform-centric, and ecosystem-centric one – is one that fits nicely into the structure and mechanics of the DSA. This centrality approach has been also embedded in the Cybersecurity Research Focus Areas Priorities, identified, discussed and established by CONCORDIA and other three (3) pilots.

From a very practical point of view, a metaphor to describe some of the various societal responsibilities that are part of the DSA is a concert hall:

The concert hall itself has to provide for a safe environment, fire extinguishers, alarm buttons, emergency exits, and trained staff. Meanwhile, this does not imply that the concert hall is responsible and liable for everything, but there is a fair and reasonable share of social responsibilities that the concert hall needs to cater for.

Inspection agencies, such as the fire brigade, elevator and building inspectors will periodically perform site checks and the like, and that those inspection agencies are overseen by competent authorities. Furthermore, the visitors will still be accountable for their own behavior while being able to trust that both the concert hall and authorities did their part to provide for a safe environment.

To a large extent, the DSA has the same – very logical and necessary – responsibilities, accountability and oversight mechanism; a transparency and accountability framework that requires online platforms to provide for a safe – digital – environment and provides new tools for both user empowerment and governmental agencies to help its citizens and support and cater for those fundamental rights and freedoms.

In short, the DSA is a framework that tries to strike the balance between those many (and in many cases on contextual level clashing) fundamental rights and freedoms and the responsibilities of online platforms on which so many depend nowadays.

#### **4.3.6. Implementing Digital Sovereignty Principles: AI Tooling Perspective**

When having had to experience a personal trauma, and becoming a victim, with ones' self-sovereignty crushed and low confidence in societal sovereignty in safety, security, trust, accountability and recourse – also towards the offenders –, does one just remain a victim or survive it and thrive through it?

If one chooses the latter, can one help others, and if so, what digital tools are available to identify, isolate and stop harassment, abuse and other misconduct, in a practical, efficient yet accountable way?

In this Digital Age, various combinations of mission-focus, digital capabilities, data and data analytics can help support these problems. Useful patterns can be identified, with data analytics including trustworthy artificial intelligence (AI). Making sure those are not biased is the main accountability principle by design, also otherwise before, during and after deployment. This is not a one-time exercise, but will need to be monitored, double-looped, configured and further optimized on a continuous basis.

However, if one takes this approach, AI capabilities can support (cyber-)security, safety and other (digital and other) sovereignty challenges and augment the positive outcome thereof. Addressing serious societal challenges, developing, and optimizing mission-based AI for accountability, being accountable for AI and balancing these out in this dynamic digital era are enablers, not problems.

#### **4.3.7. Implementing Digital Sovereignty Principles: University Lecturer Perspective**

When lecturing students on electrical engineering at a university, creating awareness, understanding and appreciation about non-functional such as cybersecurity, accountability and other digital sovereignty components is not an easy feat. Several learnings can be taken out of this, while architecting, building and operationalizing the competence centers and the network within the EU and its member states.

Seeing each university as a nucleus, generally starts with conveying technological knowledge. This also is driven by the fact that most universities are bound by the curriculum of their national department of education. However, generally, cybersecurity – or at least the non-technical elements regarding cybersecurity – are not part of the official curriculum of technical universities set by such department.

When assessing the notion of students about accountability in these digital and otherwise technical domains in general and the cybersecurity dimension in particular, it is basically

unknown. From the technology-perspective, cybersecurity initially may be relatively simple: technology is working or not, and if it has a problem one can fix it. However, this is isolated thinking and approach that does not take into account the impact and other effects each component may have on others, on the digital ecosystems it is part of, on people, society, nations, unions and digital sovereignty at large.

The main problem is a lack of awareness. If one is not aware and understands that is both part of the problem as well as of the solution, one cannot appreciate it and with that start to think about and contribute to these essentials. The interview even stated that it all starts with awareness, and it should even prevail to technological knowledge. What is expected, what can possibly go wrong, and how to build in monitoring, cure and other recover and support capabilities when things may go wrong? Working on accountability through daily studying about technology, research and practice is the preferred way. Additional or an amended curriculum, and where not possible at least colloquia, therefore, are both recommended and required.

Asking these students why they are not using the university digital workspaces and communication facilities provided but seem to prefer using a non-EU facility of which it is well-known that it conflicts with various dimensions of digital sovereignty, including without limitation deep tracing and other surveillance advertising practices, a frequently heard answer is 'everyone is using it'. This is a clear example of convenience and 'fear of missing out' prevailing over the assured trust.

It does also demonstrate that even when the individual in its persona as student is educated and made aware about non-functional such as cybersecurity, accountability and other digital sovereignty components, this does imply that such individual in its persona of mere user practices such awareness. It is an example of the multiple-persona of Dr. Jekyll and Mr. Hyde, and it is obviously wrong, yet apparently more natural than want would like it to be. This behavioral multi-persona (where there for sure can be more than two persona) is to always be taken into consideration in the domains CONCORDIA and other pilots are active in, as these are generally forgotten and go much further than the mere notion of 'the human factor'.

#### **4.4. The Code of Engagement for Threat Intelligence Sharing**

Acknowledging the sensitivities in the domain of cybersecurity and the role culture plays, especially, in relation to information sharing, T4.2 focusing on the Legal Aspects of Cybersecurity, also, led the joint activities with WP3 that resulted in the creation of a Code of Engagement for Threat Intelligence Sharing (CoE), providing initially for the sharing of information between the three actionable components of CONCORDIA platform, namely, the MISP Central, ICH respectively DDoS-CH communities.

By moving away from the traditional methods of creating symbiotic relationships such as those in the form of contracts, terms and conditions and codes of conducts, the CoE aims at connecting the adhering parties/members with the community of cybersecurity domain experts and organisations as defined under the CoE, in order to share threat intelligence in a trusted and trustworthy way, while building a future-proof community, adding to resilience and jointly and individually achieve outcomes. To this end, the CoE is intended to inform, guide, facilitate oversight, insights, trust, expectations, and understanding, and to arrange the various relationships and data flows, and set a principle-based intelligence

sharing and collaboration framework to cater for trust and boost engagement and sharing. Furthermore, the CoE is designed as a runtime an organisational living and learning operating system for the community and its members as, similarly, defined in the CoE which will be securely patched, optimized and upgraded with new features same as trusted and secure software.

Although the focus of CONCORDIA Platform for Threat Intelligence is currently on the three (3) aforementioned core actionable components, it -also- gives the ability to jointly develop, live-pilot, deploy, iterate, improve and optimize the dynamic CoE including without limitation its data- & impact-centric governance, organising each of these core components in general, and any specifics in particular. The CoE governs, thus, the engagement and collaboration with, in and between the community and its members, as well with, in and related to Platform and its respective core components and content, to the extent made available in relation to privacy, the privacy of others and related matters.

Note that, following the agreement between CONCORDIA partners responsible for the development of CONCORDIA Platform components and contributors to the CoE, namely, Siemens, DFN-CERT and SIDN, the latest version of the CoE is currently publicly available and can be found in Appendix B.

## 5. Economic Perspectives

Task T4.3 focuses on the investigation of CONCORDIA's stakeholders regarding the economic dimension of cybersecurity that concerns costs of different systems involved, mechanisms in use, and processes determined. Based on that, Task T4.3 has mapped key information and steps for cost-effective cybersecurity planning, deployment, and operation. With this knowledge obtained, a methodology to guide companies in investing in cybersecurity is provided together with solutions covering its different steps. Although the methodology steps are adjustable and can change in accordance with specific demands, they can be used, along with the different solutions provided, as an initial guide for companies that need to implement a new cybersecurity strategy or refine their current one.

Figure 5 depicts a framework [86] that includes the different phases and key issues to be considered when planning and deploying an effective cybersecurity strategy and is an overview of the guiding steps that are defined within the context of Task T4.3. The framework starts in Phase A, where all information related to the business is collected and a briefing is conducted with all stakeholders involved. Then, Phase B focuses on the security analysis and threat modeling of the business under investigation. For that, state-of-the-art tools, solutions, and approaches can be considered, such as the SEconomy framework proposed in Deliverable D4.1 or specific penetration tests. Subsequently, with the relevant security information at hand, Phase C consists of the definition of cybersecurity requirements, the mapping of processes that must be modified or created within the business and the definition of training required to implement, deploy, and operate the cybersecurity strategy.

After all information is mapped and all relevant cybersecurity requirements are defined (e.g., what is the main goal, what is an acceptable level of protection, and which risks can be assumed), the Cost Management phase (Phase D) starts. In this phase, cybersecurity costs are estimated, and the optimum investment amount is defined. For that, a parametric estimation is conducted to determine costs in terms of time and resources required. This

enables the implementation of cybersecurity planning and deployment. The current step uses the business's historical data and information of successful projects that have been implemented in companies with a similar environment (e.g., sector and number of employees). Therefore, the parametric estimation supports estimations that require a certain level of granularity of resources and time.

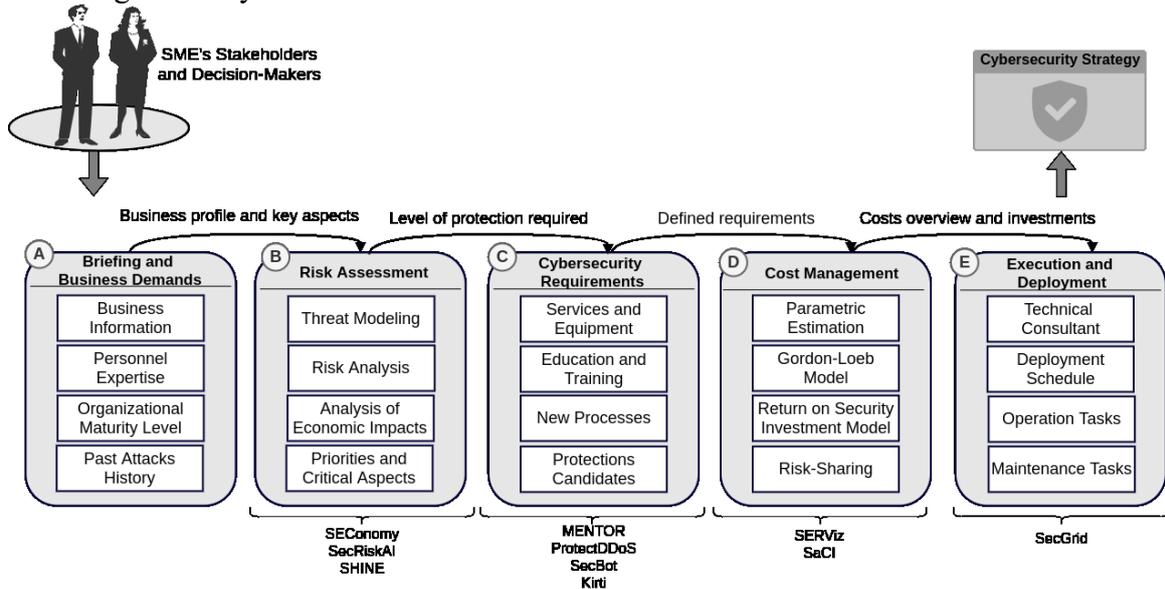


Figure 5: The Framework Proposed [86] within the Context of Task T4.3 to Map Main Information and Phases for Cybersecurity Planning

As SMEs typically do not have a lot of experience with cybersecurity-related aspects-, it is possible to use both (a) information from other companies and partners with similar characteristics and sectors, and (b) expertise from other IT projects that show costs to deploy, train personnel, and operate new solutions. This approach, together with the different models presented below, is considered to be highly effective and useful when employed as an estimation tool providing a very reasonable level of accuracy. Examples of aspects to be considered for such a parametric estimation (*i.e.*, for the estimation of costs and time) of cybersecurity projects include:

- Collection of historic and market data on cost and time requirements to implement similar protections and training;
- Determination of the maturity of the team to lead and implement the project;
- Determination of steps that are critical for the success of the project, which cannot be excluded from the budget available; and
- Definition of the number of solutions to be deployed and the identification on how large the infrastructure is, which needs to be protected (*e.g.*, number of end-points, computers, and network devices).

Taking the above information and applicable metrics into account, it is possible to apply the parametric estimating formula to each of these relevant metrics to achieve a measurable view on a cost estimation of cybersecurity, which can be correlated with the optimum investment and Return On Security Investment (ROSI). Such a parametric estimating formula is defined in Equation 1.

$$E_{Parametric} = \frac{A_{old}}{P_{old} \times P_{curr}} \text{ where,}$$

$$A_{old} = \text{Historic amount of cost } \forall \text{ time}$$

$$P_{old} = \text{Historic value of the parameter}$$

$$P_{curr} = \text{Value of that parameter } \in \text{ the current project}$$

Equation 1: The Parametric Estimation Formula [87]

Still within the Cost Management phase, it is important to determine the maximum amount of funds to be invested in cybersecurity based on the business's value and data. For example, in some instances, it is more adequate to assume risks than to invest a large number of funds in protecting non-critical systems or system components. In order to obtain this value, the proposed framework considers the Gordon-Loeb model [4], one of the most well-accepted models for cybersecurity investments.

Gordon-Loeb determines that the investment in security should not exceed 37% of the potential loss ( $d$ ). The investment relates to how much the system is valued ( $\lambda$ ), how much the data/system is at risk ( $t$ ), and the probability that an attack on the data/system is successful ( $v$ ). Equation 2 describes how to use this information for this calculation.

$$\text{Investment} = d \times 0.37, \text{ where}$$

$$d = \lambda \times t \times v$$

Equation 2: The Gordon-Loeb Model [4]

After obtaining the optimum amount of investment in cybersecurity (*i.e.*, the Gordon-Loeb calculation), the next step consists of determining which are the candidate solutions (*e.g.*, firewalls, antivirus, and cloud-based services) and strategies (*e.g.*, employees training and backups) to be applied, as described in previous phases of the framework (*i.e.*, Cybersecurity Requirements), based on the budget available. For that, as proposed in [88], recommender systems, such as MENTOR, can be used together with other methodologies based on the business's technical know-how.

After these solutions are mapped, the next step is to perform the ROSI [89] analysis for each one of them. This step includes, for example, the calculation of ROSI for investment in solutions (*e.g.*, firewalls, antivirus, and cloud-based services) and other tasks (*e.g.*, training and backups). The ROSI model is introduced in Equation 3, and is considered satisfactory (*i.e.*, the investment is recommended compared to the potential loss), if the equation results in a number higher than 1.

The ROSI assess whether a solution is worth the investment or not. In order to do so, ROSI takes into account the Annual Loss Exposure (ALE), the mitigation rate, and the cost of the investment to assess. For that, the Single Loss Exposure (SLE) and the Annual Rate of Occurrence (ARO) have to be considered, which describe the estimated cost of a security incident, respectively (*e.g.*, a data breach or a DDoS attack in the business), and the estimated annual rate of an incident's occurrence (*i.e.*, based on the historical data and threat modeling, which are the probability of being attacked). All of this information is

investigated during the Phases A, B, and C. Furthermore, the cost of the investment and the possible proactive mitigation (*i.e.*, how much of the attacks can be avoided or mitigated by implementing the solution) have to be mapped and considered for an accurate ROSI calculation.

$$ROSI = \frac{(ALE \times MitigationRate) - CostoftheInvestment}{CostoftheInvestment}, \text{ where}$$

$$ALE = SLE \times ARO$$

Equation 3: The Return On Security (ROSI) Model [89]

The last phase of the proposed framework is defined as the Execution and Deployment phase. Earlier phases have already produced the artifacts and information that are required for managing the execution and deployment of the cybersecurity strategy with a clear view of its risks, costs, goals, and success rate. In the light of this information, the business can define requirements for an external technical consultant or schedule and implement the technical tasks required for the effective deployment and application of the newly adopted cybersecurity strategy. Also, operation and maintenance tasks have to be described within this last step in order to not only reach a good protection level, but also provide an efficient plan to manage and operate the entire set of countermeasures, which might require additional training, employees, and equipment that fits the budget as previously defined in the cost of the cybersecurity strategy.

Task T4.3, in order to address the different significant challenges and steps, has been researching and developing various solutions. Table 2 summarizes the solutions proposed within project years 1 to 3. The current report will not present solutions that were already discussed in Deliverables D4.1 and D4.2, and thus it will focus on cyber insurance, reputation systems and a Service Level Agreement (SLA) audit, and an ML-based risks assessment of companies.

Finally, all these solutions are integrated into a unified architecture that covers the phases and steps highlighted by Task T4.3 within Figure 5. The remainder of this section proposes and discusses new approaches (*i.e.*, SaCI, Kirti, and SecRiskAI) that already address not yet in detail tackled facets by early solutions within the set of economic aspects of cybersecurity.

Table 2: Summary of the Different T4.3's Solutions and Steps of Cybersecurity Planning Addressed

<b>Solution</b>	<b>Description</b>	<b>Phase Addressed of the T4.3 Framework</b>	<b>Reported</b>
SEconomy	A framework for risk assessment from an economic perspective	Phase B	M12, D4.1
MENTOR	A recommender system for protections	Phase C	M24, D4.2
ProtectDDoS	Integration of MENTOR with a frontend for recommendation of protections against DDoS attacks	Phase C	M24, D4.2
SecBot	A conversational agent for cybersecurity planning and management	Phase C	M24, D4.2
SERViz	A visual tool for cybersecurity investments based on the ROSI	Phase D	M24, D4.2
SaCI	A blockchain-based cyber insurance model	Phase D	M36, D4.3
SecGrid	A platform for the analysis and visualization of cyberattack traffic	Phase E	Supplementary service within T3.2
SecRiskAI	A ML-based tool for risk assessment in companies fully integrated with MENTOR	Phase B	M36, D4.3
SHINE	An economic module for the SecGrid platform, which allows for economic information sharing	Phase B	Supplementary service within T3.2
Kirti	A blockchain-based reputation and SLA audit system for the cybersecurity market	Phase C	M36, D4.3

### 5.1. Cyber Insurance (CI) Market and Models

The Cyber Insurance (CI) market is still in its infancy, but it is growing fast [90]. Novel models and standards for this particular insurance market are essential due to modern IT and the fact that insurance providers need to create suitable models for customers [91]. In 2020, Munich Re estimated the current CI market roughly at € 8 billion in premiums [92]. The CI market, therefore, constitutes less than 1% of the overall insurance market. However, the massive growth of the CI market [93] is a strong driver for insurance companies to put cyber insurance products in focus to compensate for the otherwise stagnant growth of the overall, and even sometimes considered saturated insurance market.

Regarding its structure, a functioning CI market needs two clearly defined sides: demand and supply. The demand side refers to companies that are willing to acquire insurance, so-called insured (*i.e.*, a person or organization covered by insurance). The supply side, also known as insurers, is responsible for providing insurance through an underwriting process

[94]. Moreover, the supply side can also be broken down into three parts: brokers, insurers, and reinsurers.

### 5.1.1. Overview of Cyber Insurance Steps and the Framework Definition

A literature review and interviews with CI underwriters were conducted to identify the most relevant information for CI models. One of the main goals of such work is to elaborate a practical and useful framework that unifies and covers relevant approaches within the CI context. In this sense, it is possible to classify and understand current models and frameworks not only on the understanding of the market and its stakeholders, but also on the definition of the premium and different external events that affect the *status quo* of the CI market. Therefore, the structure of the proposed CI framework considers three essential pillars: (a) Market Model, (b) Premium, and (c) Environment. All of these steps and information relevant to the framework are detailed within Figure 6.

As shown in Figure 6, the framework indicates that a first analysis (depicted in the top left corner in shades of green) of the Market Model has to be carried out, defining and identifying the Business and Risk model. Once this step is concluded, one can continue with the aspects that concern the premium considerations (depicted in the bottom left corner in shades of blue). In the Premium pillar, the framework considers all contractual and calculation issues in which the customers and insurers will be involved as a result of the underwriting process. Finally, in this CI context, a third and last pillar called Environment (depicted in the right in shades of purple) highlights the external factors that affect both pillars mentioned before: the premium and the market model.

As initially stated, this framework was mainly elaborated based on exhaustive literature research. However, a validation process was also carried out by interviewing experts in the CI field. The feedback provided from the interviews conducted was, in general, positive, since the interviewed experts all agreed on the level of completeness and the detail of the framework. Nevertheless, they pointed out selected remarks on the Market Model and Environment that they considered important to mention explicitly. These include security standards, reinsurance, and external malicious attacks. These proposals were included, too, and are highlighted within Figure 6 in yellow.

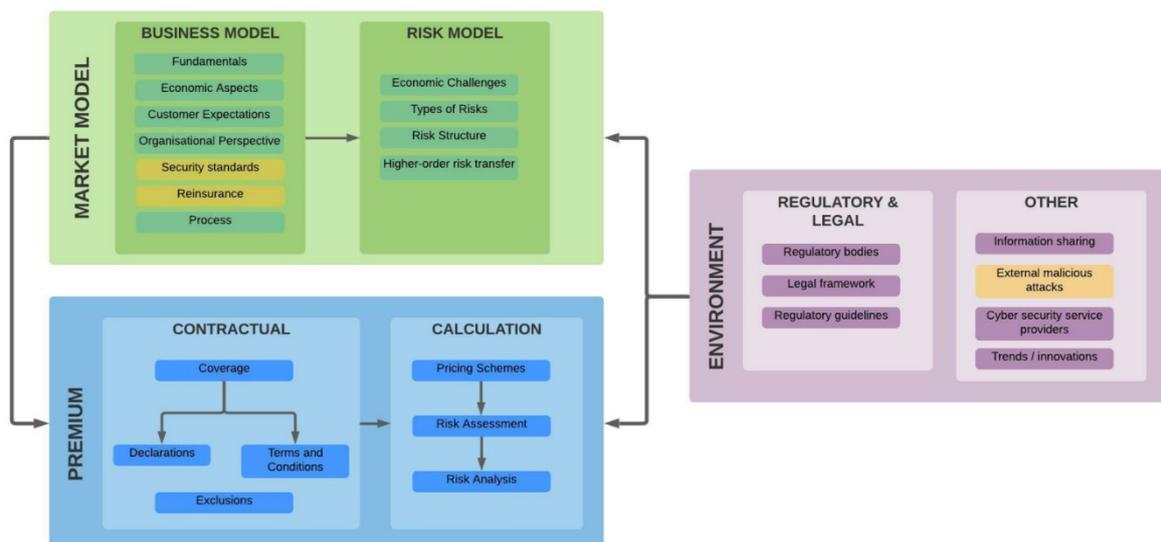


Figure 6: Practical Framework for Cyber Insurance and Reinsurance

### 5.1.2. Stakeholders and Relationships

A first move toward the elaboration of frameworks or models for the CI market is the identification of different stakeholders and actors, together with their interactions. Therefore, this subsection identifies all organizations and entities directly or indirectly affected, or who have specific interests within a CI model. Thus, key questions were asked to understand the participation of different stakeholders. These questions are defined as follows:

- Who are parties affected within the CI model?
- Which processes are affected within the CI model?
- Which other entities, besides customers and insurers, are affected by the CI model?
- What is the interaction or connection between entities?

The final result is an entity-relationship model that maps the CI model's stakeholders, actors, and key concepts. This entity-relationship diagram is presented in Figure 7. As it can be seen within the legend, red boxes represent key stakeholders, blue and oval boxes represent other entities, concepts, or attributes. White diamonds explain the relationship between them. Finally, the different types of arrows represent cardinalities. Each mapped entity is described in detail below.

- **Regulator:** The main task of the regulator is to oversee the work of the insurance and reinsurance companies. The cardinality between them is one or many to many.
- **Reinsurance company:** Reinsurance companies play a crucial role in today's CI's context. Their task is to reinsure insurance companies by taking part in the risk. The association here is also many to many.
- **Insurance company:** One of the central stakeholders in the CI model, insurance companies, has two entities that closely collaborate with them. On the one hand the underwriters that work for them and the cyber security vendors that work with them. Both of them help the insurance companies reach the customers.
- **Underwriter:** As mentioned before, the underwriters work closely with the insurance companies and their main task is to carry out the underwriting process, which gives, as a result, the insurance policy for the potential policyholders (*i.e.*, customers).
- **Cyber Security Vendor:** A cyber security vendor takes an important role in the model since they are in charge of advising and suggesting the customer regarding their security standards. This approach helps both, insurers, and customers. On the one hand, it mitigates the risk that insurers will take from the insured company. On the other hand, it reduces the premium that customers will have to pay due to best security practices.
- **Policyholder/Insured/Customer:** Considered another central stakeholder in the CI context. Customers are assigned a risk profile by the insurers, in which this risk profile is a criterion needed to elaborate the premium calculation and later on create the premium schedule which is part of the insurance policy that the customer will hold. This insurance policy is mainly developed and customized according to the customers' needs (*e.g.*, coverage for business interruption, and data breach). It can also include other factors (*e.g.*, limits and sub-limits) and exclusions that describe what is not included in the contract.

- **Broker:** Finally, brokers have the task to manage the portfolio of the customers from insurers and to sell the insurance policy to them. It is also worth mentioning and highlighting the key role that CI brokers play currently in the underwriting process. As our interviewees indicated, brokers take over some of the key risk assessment tasks and match the prospects to a CI product. The current CI market, where heterogeneity, information asymmetries and complexity play a central role, is one that creates a sizeable opportunity for different types of brokers.

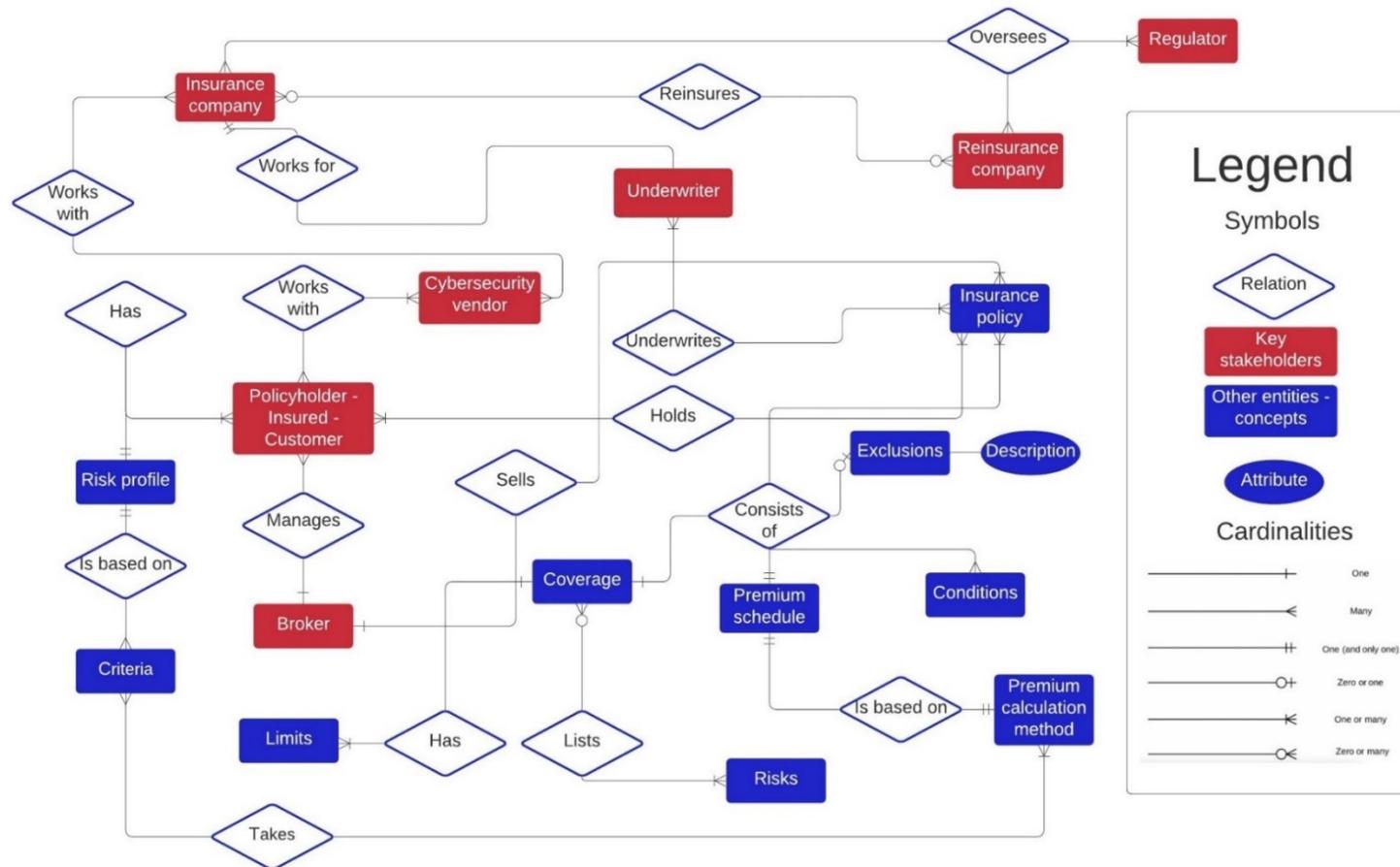


Figure 7: Cyber Insurance Stakeholders Entity-Relationship

### 5.1.3. SaCI: a Blockchain-based Cyber Insurance Model

In order to support the adoption of novel solutions for CI, a refreshing approach called SaCI (Smart Contracts for Cyber Insurance) is proposed [95]. SaCI handles different demands of cyber insurance in order to create a simplified, trustworthy, and automated process for cyber insurance contracts. For that, SaCI describes a JavaScript Object Notation (JSON) file structure to store relevant information about the contract and to translate it to SC code within well-defined functions allowing for interactions between customers and insurers. Therefore, the SaCI allows for the (i) payment of premiums and contract updates, (ii) request of damage coverage and dispute resolutions, and (iii) check of contract information and its integrity, whenever it is required (e.g., in case one of the parties involved are not following the agreement defined).

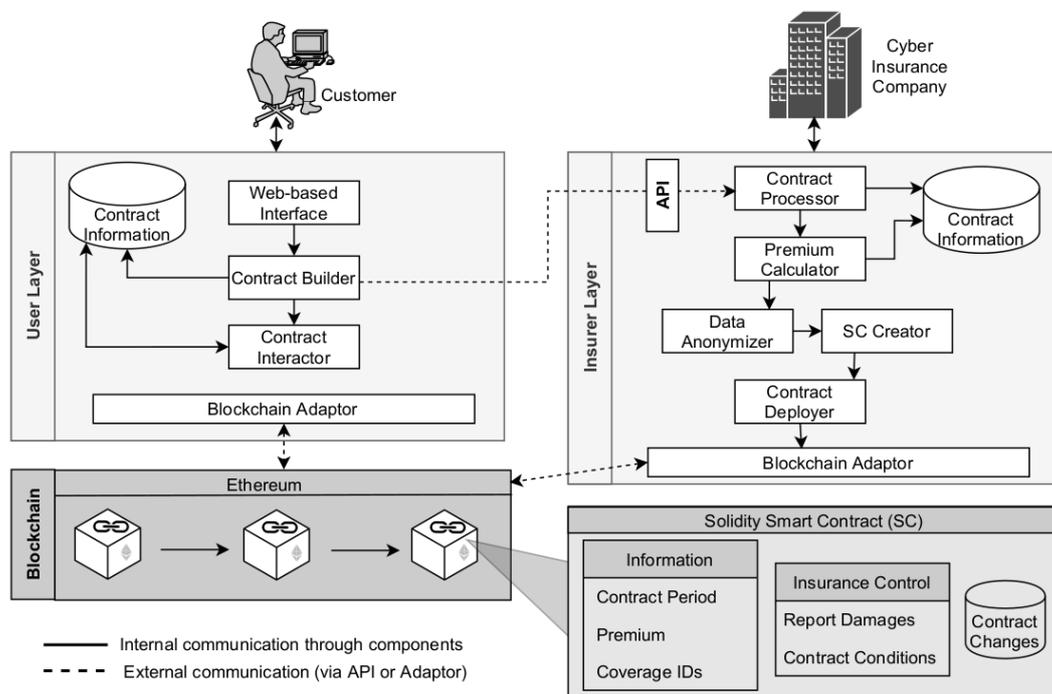


Figure 8: The SaCI Architecture

Figure 8 depicts the architecture of SaCI and its components. The architecture shows the two different stakeholders (i.e., customer and cyber insurer) at the top and enables the interaction with the system using those components running on their respective layers (i.e., on their own infrastructures). The *User Layer* is composed out of a Web-based interface, with which the customer can access and add all information related to business and demands. A summary of the relevant information considered by the approach is presented in Table 3. This information is forwarded to the *Contract Builder* in charge of mapping this information into the defined JSON format. The respective JSON file is sent to the *Insurer Layer* using the SaCI’s Application Programming Interface (API).

Within the *Insurer Layer* the *Contract Processor* reads information from this JSON file and stores a copy of all contract information. The *Premium Calculator* estimates the premium for this contract’s coverage according to the information provided. While SaCI does not focus on an optimal premium calculation, it provides relevant information in a standardized format, e.g., as input for a base rate pricing in which modifications for the calculation can be accommodated according to insurer preferences.

After the premium calculation, the *Data Anonymizer* component is in charge of removing from the contract all information that can be critical to identify the company and its risks. This is essential before deploying the contract within a public Blockchain (BC) (e.g., Ethereum, Cardano, or Tezos) because all information in the SC is visible to any peer in the BC. The *SC Creator* uses all other information to transform the JSON file into an SC based on a previously defined format (e.g., Solidity code) and fills in missing information in those fields mapped. Finally, the contract is deployed on the BC and is available for interactions between all stakeholders (Actors) involved.

Table 3: Contract Information

Category	Description	Example
Business Information	Standard information about the company, which is not relevant for the premium, but which is needed to identify the company.	Company name, Company address
Contract Constraints	Information about the non-technical constraints of the contract, which have to be completely defined in each contract.	Duration of the contract, Payment frequency
Company Conditions	Non-technical information about the company's business number, which affect the premium.	Yearly revenue, Number of employees
Company Security	Information about the measures of the company to increase its cyber security as well as different metrics to measure it.	Risk assessment metrics, attack history, security software, security training
Company Infrastructure	Information about the hardware and software used by the company.	Used technologies, Critical data amount
Contract Coverage	Information about what attacks and impacts are covered by the contract and by which conditions.	Ransomware: Business interruption: coverage at 50%; data breach for third-person damage: coverage: at 100%

In order to define the relevant information for the creation of the CI contract, and consequently, the SC, necessary information was determined based on the related CI market. Table 3 provides an overview of these main categories considered by SaCI. Every characteristic demanded by a customer is assigned to one of these categories. Note that this type of information has to be provided by customers, which might result in "inaccurate" information and can be impacted by companies' biases, such as metrics related to risk assessment and threats impacts.

The business information contains standard information about the company, which is most likely to be known publicly. This information is needed to identify the company, but it is not relevant for a premium calculation. Basic conditions (e.g., contract duration) are stored in contract constraints. Company conditions comprise all non-technical characteristics and mainly include information about business numbers. The following two categories (i.e., security and infrastructure) are significantly related to each other and they encompass all technical characteristics. With the information of these two categories, the probability and partially the impact of a successful attack can be estimated to better understand all risks by both actors.

While the company security category describes different metrics about security deployed and measures are taken to improve the security, the company's infrastructure includes all information of hardware, software, and technology as well as about critical parts of those. Finally, within the contract coverage category, details about every contract's coverage are stored in an unlimited list. For every attack, the costs covered and possibly other constraints of the specific coverage (e.g., maximum indemnification of insurer) are defined. The contract coverage is the most important part besides the risk assessment to calculate the premium.

Table 4: Examples of SaCI Functions Implemented in the SC

Function	Actor	Parameters	Description
payPremium	Customer	-	Pays the premium converted in Ethereum's currency, increases contract's time of validity
reportDamage	Customer	uint date, uint amount, string type of attack string logfileHash, uint damage id	Creates a damage <i>struct</i> on the contract
acceptDamage	Insurer	uint damage_id	Accepts damage with ID and pays out reported damage.
acceptCounterOffer	Customer	uint damage_id	Accepts counter offer, which is paid out automatically.
resolveDispute	Customer	uint damage_id	Resolves a dispute about a damage reported, when a solution is found off-chain.
UpdateContract	Both	uint new_premium, string new_file_hash	Makes a proposal to update the contract.

Listing 1 shows an example of a contract coverage against two different threats (e.g., business interruption due to a DDoS attack and third-person damage due to a data breach) defined in the JSON file's descriptor. Finally, upon entering information of all categories, the content can be forwarded to the *Premium Calculator*, which will calculate the premium and inputs the SC generation.

```

"contract_coverage": [
  { "name": "DDoS",
    "coverage": [{
      "name": "Business Interruption",
      "coverage_ratio": 100,
      "deductible": 1000,
      "max_indemnification": 300000 }]}],
  { "name": "Data Breach",
    "coverage": [
      { "name": "Third-party damage",
        "coverage_ratio": 100,
        "deductible": 1000,
        "max_indemnification": 300000 }]}]}]

```

Listing 1: JSON of a Contract Coverage

At this point, the contract is deployed on the BC and can be accessed by the insurer and the customer utilizing functions available in the contract (*cf.* Table 4). This list is not exhaustive and other functions are available in the proposed SC, too, all details are available within the implementation.

After the premium is paid and the contract is enacted, the actors can interact. For instance, in case an attack happened, the customer can call the *reportDamage()* function to ask for refunding or help. The insurer can accept or deny the coverage requested. If accepted (*i.e.*, *acceptDamage(id)*), the payment is made automatically via the SC according to what was defined previously in the contract. Note that the customer can also provide a hash of a log file as proof of the attack. This hash is also stored in the BC to further enable an integrity check. At the same time, the file itself has to be stored off-chain, especially inside the contract information datasets maintained by both actors. *If the parties cannot reach a conclusion, counteroffers can be made by the insurer (i.e., payment for a specific loss, but not for all financial losses).*

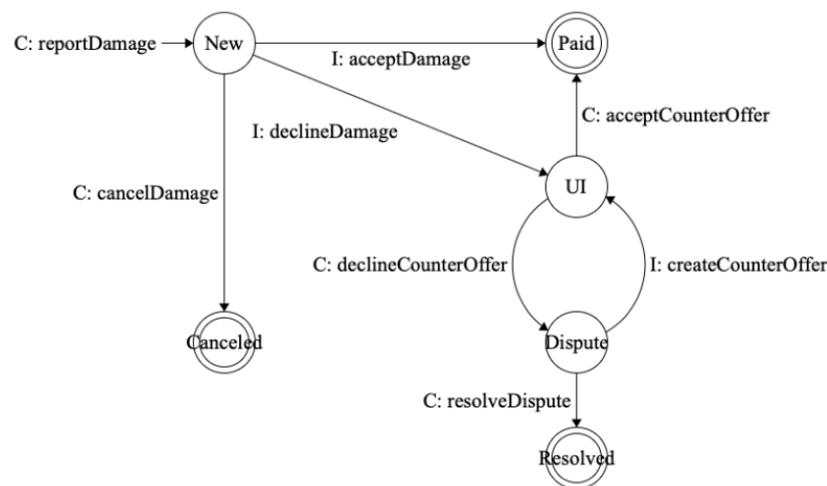


Figure 9: State Diagram of SaCI Interactions

Figure 9 shows the state diagram of possible interactions after a *reportDamage()* is called by the customer. The report damage process has one of the following states: New, Paid, UnderInvestigation, Dispute, Resolved, or Canceled. This diagram exemplifies the different functions' use (*e.g.*, *reportDamage()*, *acceptDamage()*, and *acceptCounterOffer()*) to claim a settlement.

The Canceled status is an ending state, reached only if the customer cancels the request. Paid status defines that the insurer accepted to cover the damage, and it was automatically paid. If the contract has a lower balance than the value to pay out, the insurer has to transfer funds to the contract, when accepting the coverage. If the insurer declines the coverage payment, a reason is provided, and a counteroffer is issued. If a counteroffer is not possible to be offered at that time, the status is defined as UnderInvestigation, which means that further manual investigations have to be placed off-chain before a counteroffer can be placed.

If the insurer provides a counteroffer (*e.g.*, a lower amount than the initially requested compensation for that incident) and the customer does not accept it, the state changes to *Dispute*. This refers to the fact that no agreement has been reached yet. Either the insurer creates a better counteroffer, or the two actors have to solve the dispute off-chain for which a third party may be considered. If the dispute can be solved, the final status of *Resolved* will be achieved. Using the SC function called *getAllReportedDamagesWithStatus()*, all

reported damages with a specific status can be returned, which also allows verifying the history of past interactions, *e.g.*, accepted, declined, and under investigation coverage requests.

A prototype of the SaCI was implemented using Python as backend language and Solidity for the SC development. The Ethereum BC running on the Ganache testbed has been used for the deployment and tests of SC functionality. For SaCI's API, Flask was used in its latest version. Finally, for the off-chain storage, the prototype uses SQLite. The source-code and all documentation are publicly available<sup>130</sup>.

## 5.2. Cybersecurity Ecosystem Benefits

The European Cybersecurity Competence Centre (ECCC), together with the network of National Coordination Centres (NCCs), and the Competence community (CC) can be considered as a specific type of a multi-organisational structure aiming at strengthening the capacities of the cybersecurity. While the full governance model of this structure is still under construction, we can already make some abstraction and address this structure, and especially the “competence community” part, as a kind of networked organisation or an ecosystem.

In this context we define ecosystem as “a system of people, practices, values, and technologies in a particular environment” (see CONCORDIA deliverable D6.3). The ecosystem includes roles, tasks, and relationships, which could be customized for different layers or even different member states (see inter-pilot focus group on ECCC and governance models).

Unlike the concept of a network, ecosystem also brings dynamicity, since different alternatives need to be considered also from the economic perspective (*e.g.* reuse of software components, shared resources such as lab, and scale-up of new solutions). Several economic theories of the collaborative and cooperative generation and consumption of new value apply here, and the work should start with understanding the context, modelling of economic (*e.g.* cost-benefit) assumptions, planning, implementation, value creation, and assessment. At this stage, not many details about the governance of financial provisions are revealed about the ECCC, which will be located in Bucharest, or the other two layers (NCC, CC), so this theoretic study will be based on lessons learned from the other similar value co-creation experiences.

In CONCORDIA, there are directions given by Industrial Strategy Committee (ISC) that takes ecosystem/networking effect as one of the parameters to support innovative solution building in the future, through Cybersecurity competence community. In WP5, exploitation results (ER) have been ranked by ISC not only according to their unique value proposition, market demand or technical maturity, but also according to their “network effect”, which justifies why the exploitation should be done through an ecosystem approach, such as the case of competence community. This applies, for example, to DDoS clearing house, certification scheme or Threat Intelligence Platform. In our case, we focus on Financial Threat Intelligence Platform (F-TIP) and Financial Cybersecurity Threat Intelligence (F-CTI) process in general.

---

<sup>130</sup> <https://gitlab.ifl.uzh.ch/franco/saci>

Most of the work described in this chapter, however, is theoretical work applicable not only to F-CTI, but to any exploitable result (ER) whose economic benefit relies on wide ecosystem support or adoption. The more you share, more benefit there is for all. This looks like a straightforward and intuitive message, but hard to measure quantitatively and qualitatively. This is also the reason why we prepared two events with the financial sector stakeholders, scheduled for November 16<sup>th</sup> and December 14<sup>th</sup>, 2021. While outcomes of these meetings will be reported in task T2.2 and WP5, the suggested approach to measure economic benefits of sharing and estimating value of data services, data sources and data itself, is described here.

Finally, we will also try to apply our approach and tools for real-time risk assessment in order to measure benefits of financial cybersecurity threat intelligence (F-CTI) sharing. The real-time approach described already in D4.2 is based on use of data from security information and event management (SIEM) tool but can also use another type of inputs. Any other risk assessment approach can also be used to estimate benefits of threat intelligence sharing.

### 5.2.1. Cybersecurity Ecosystem Specificities

Some stakeholders in cybersecurity ecosystem, similar to what already happens in four pilots of competence community (ECHO, SPARTA, CSEU and CONCORDIA) will have both contributor and beneficiary role, being present simultaneously on the supply and demand sides (*e.g.*, the telecommunication use case within CONCORDIA). Solutions are supposed to be reused, while others will profit what in CONCORDIA WP5 was called “network effect”. As a matter of fact, in 2020 a total of 30 exploitable results (ERs), across 27 partners, has been presented to CONCORDIA industrial strategy committee (ISC) for the ranking according to four criteria, one of them being community and network “orientation”. These ERs, for example, include platforms whose value depends on data sharing or the number of stakeholders participating. From this perspective, we can also investigate links to “platform economy”.

All these particularities will shape “cybersecurity ecosystem economic model”, and the aim of the following chapters is to list some existing experiences and identify factors or challenges that would be needed to take into account when shaping governance and evolution of this forthcoming ecosystem.

### 5.2.2. Related Work

Business ecosystems [96] [97] are structures where large companies can co-evolve their skills together with academic partners and smaller, more agile companies. Unlike CC, these are centred around one large company although it also builds upon the idea of value creation by putting together different assets and skills. This process is often non-linear as in CC, but the configuration is not that complex, and stakeholders are mainly from the supply side. Partners are expected to complement each other, and value also stems from the linkage. In addition, when new organizations enter this ecosystem, they should adapt to the value network, which might represent a constraint or even weakness. Value co-creation in the context of cybersecurity has been studied or described previously in EU-funded projects, for example in WITDOM, where a paper [98] shows how to integrate practical co-creation processes into Security-and-Privacy-by-Design methodologies.

Network effects that increase the value often enable a single company to take large market shares [99], with well-recognized internet services such as advertising, social networks and search being the most prominent examples. As a result, so-called scaling benefits arise. Depending on the type of application, the added value benefits users in different ways and depends on openness and centralisation [100]. In the open web, the value grows for everyone, although smaller entities have it more difficult, while in more closed applications, such as social media, the value depends on how many other customers that service has.

When it comes to business model that are especially suitable for cybersecurity ecosystem, we also refer to SAINT project [101] which delivered and analyzed a set of models including the labelling and certification model, the crowd sourcing model, the collaborative model, or the education and awareness raising model, among others. These models address the cybersecurity challenge from a systemic perspective, and according to the authors they examine all possible interactions dynamics and scenarios that fit into the cyber-ecosystem. Besides model dynamics, they also discuss the incentive flows that give rise to the observed dynamics and new ways to adjust, change or disrupt existing incentive flows in order to increase the overall level of security in the cyber-ecosystem. The role of regulatory approaches was explored while qualitative social science methodologies were used together with comparative analysis of the failures of current cybersecurity solutions, products and models. Econometrics (economic measurement) was also used with a set of indicators to prove the economic theory and support the economic model of cybersecurity in general.

As mentioned before, the CC governance is still under construction, but in pilots we already proposed to introduce elements such as the monitoring of value network effectiveness and efficiency. It should monitor capability for scaling and capacity utilization, rapid identification of members that do not bring in value and can be excluded, reciprocal interdependence between members, members acting as mediators or “glue” for a value proposition, gaps, and challenges related to the long-term cybersecurity goals, specific industry configurations, failure to synchronize activities or “re-inventing the wheel”, excess of effort put into overhead activities, matching and reconfiguration, missing value elements and others.

When it comes to ecosystems with focused objectives, such as data sharing, some of these issues have already been treated elsewhere. ENISA conducted a study on Cooperative Models for Public-Private Partnership (PPP) and Information Sharing and Analysis Centers (ISACs)<sup>131</sup>, collating information on best practices and common approaches.

In October 2021 ENISA, ECSO and four pilot projects (CONCORDIA, SPARTA, CS4EU, ECHO) submitted four recommendations to the ECCC, as a result of long consensus process about the future priorities and assessment of coverage:

- Accelerate the investment in the development and production of cybersecurity products and services resulting from EU research activities
- Consolidate a vision for the development of cybersecurity competencies across EU communities
- Incorporate the human and societal dimensions into cybersecurity
- Capitalize on the results of EU funded projects

---

<sup>131</sup> <https://op.europa.eu/en/publication-detail/-/publication/597dee0f-2285-11e8-ac73-01aa75ed71a1>

These strategic directions need to be further enhanced and maybe fine-tuned for specific target stakeholders, for example start-ups and SMEs. Only 20% of SMEs in the EU are highly digitised. Addressing economics of security in priority domains such as smart energy, smart health is another possible direction, while improvement of competitiveness of local economy, for example by stimulating cost-efficient instruments for growth, transfer or creation of value networks, should also be considered.

### 5.2.3. Gaps and Challenges

Some gaps and challenges have already been identified in the first year of CONCORDIA, and these apply also to economic issues in ecosystems, such as:

- The gap between the top-down policy or market issues and bottom-up research and innovation: Although there is an aim to align industrial strategy and policy priorities with generation of innovative ideas, there is still a need to improve policy-market-technology-society alignment, as well as embed economic issues in the ecosystem
- The gap in territorial coverage, capacity and maturity in EU: While many concerns are raised about “fragmentation of EU cybersecurity market”, there is a noticeable absence of stakeholders from some member states in what is currently considered as “competence community (CC)” (four pilot projects and ECSO)
- The challenges related to EU cybersecurity ecosystem and stakeholders outside of EU
- Diversity of stakeholders, in terms of type and size (demand vs. supply side, academy vs. industry, small vs. large organizations, etc.)
- Dynamics of relationships that have a direct impact on trust, and in consequence on economics

### 5.2.4. Stakeholder Analysis

Stakeholder analysis in cybersecurity ecosystem goes further than only looking at the supply and demand side, or the inclusion of “other” external stakeholders, such as policymakers, certification and standardization bodies or legal organizations. Segmentation could and should take into account the current level of maturity, territorial approach, cultural differences, size of organizations, risk-appetite, and many other parameters. Collaboration and cooperation can be analyzed from several perspectives, from co-design of solution to service co-delivery. Less visible issues and challenges, such as SME networking, where supply-side SMEs could complement each other, should also be investigated from an economic angle. Growth and evolution of ecosystem (see for example, how CONCORDIA expanded in three years), and the motivation for diverse stakeholders to collaborate and cooperate (*e.g.*, Deliverable D3.1 and D3.2 on incentives for data sharing), have also be analyzed.

Besides complementarities and cooperation, other value drivers should be considered in the economic models for cybersecurity ecosystem, such as efficiency, avoiding vendor lock-in, or digital sovereignty. Value network reconfiguration might be needed when addressing technology acceptance or user adoption.

The technology provider group could be expanded to other providers (external to the current participants of the four pilot projects, or the initial CC) that could replace one of the existing technologies or connect them to the different environments. Research groups (universities, institutes) might need to collaborate with members which provide consultancy services to enable the transfer of knowledge to the industry or the creation of new start-ups. Open-source and other related EU communities in digital technologies (e.g., GAIA-X, DAIRO, FIWARE, and AIOTI) can contribute to the adoption, the further development and the sustainability of the ecosystem. Standardisation and certification bodies, individual investors, business angels, governmental organisation, incubators, accelerators, innovation centres, professional associations of cybersecurity practitioners and citizens are among stakeholders whose role in the economic model of the ecosystem is also to be considered.

Collaboration between stakeholders in an ecosystem may adopt various forms, depending on the context. Project or action types include contracted work, to work out and transfer rights to know-how or a prototype, consortia or partnerships, smaller expert and consultancy services, permanent cooperation structures, industry-specific or sector-specific associations, spin-off companies etc. Various factors in the choice of a cooperation model are the pool of funds and equipment available, configuration of teams and tasks, personal motivations of the persons involved, appropriate documenting and bureaucracy, protection of IP, etc.

### **5.2.5. Strategies to Stimulate Production of EU Cybersecurity Technology in an Ecosystem**

Proposed strategic directions for ECCC include cybersecurity marketplace, support services for transition from research into the development and what has been named “research and innovation platform”.

One idea is to use CC marketplace as the single-entry point with the emphasis on early product and prototype visibility to reach larger audience quickly. The value proposition of such a marketplace needs to be worked out, but it could basically create an environment for the conversation between demand and supply-side in the EU cybersecurity market, eventually leading to better and more mature products, with services (e.g. assessment, testing, deployment, integration, training) to be found in the same marketplace. “Try before buy” or “test before invest” (for start-ups that look for investors) services could also be reflected in marketplace, as well as a range of other free or trial business processes that could serve as a “hook” to sign up new customers, also outside EU.

Rationale for “ecosystem” based model is that it fits demand uncertainty & fragility. For example, there is little certainty regarding the window of opportunity, as the cybersecurity technology moves very fast, or the length of time that will elapse between the prototype launch and the development of meaningful or scalable demand from EU users. Early-stage users and demand tend to be particularly fragile. Pioneer adopters do not have the testimonials or references of existing operational environment users, as evidence or proof of value (PoV). These PoVs or “ecosystem trials” might need subsidy models involving the assumption that demand will grow after successful adoption from these “pioneers”. However, it is likely that some less profitable research or cybersecurity segments will have a gap in ecosystem revenue, while some node operations may be rendered unsustainable, or potentially destabilizing. This is where the governance mechanism should follow predefined rules or policies.

When it comes to “transition from research to market” some strategies from pre-commercial procurement<sup>132</sup> might be used when potential customer is ready to buy one of the packages based on research project prototype. Dossier could be prepared to describe as many details as possible related to the specific use case or business opportunity, including related offering with project results, draft financial conditions, list of concerned parties and any other information that the demand side customer considers important to realize the opportunity. In case of some brokers, such as Digital Innovation Hubs (DIH) or Chambers of commerce that might act on behalf of SMEs, these arrangements can include some sort of partnership or discount, as well as pre-investment agreements.

Finally, when it comes to “research and innovation platform services”, in case of CONCORDIA, there are already some services offered for free to CONCORDIA community, such as the possibility to test technologies or the catalogue of online training offerings. The project also addresses limitations and barriers when it comes to adaptation of cybersecurity to the needs of SMEs and start-ups, such as the lack of expertise (CONCORDIA training), financial resources (CONCORDIA virtual lab), or optimisation of the solutions to their needs and scale (CONCORDIA experiments). Experiments for and by start-ups could increase chances of both demand and supply side start-ups to leverage on EU funds and expertise that is available in CC. Beyond the support for integrating specific cybersecurity technologies in the processes and products created by start-ups and SMEs, there is also significant business potential for European cybersecurity start-ups and SMEs in showcasing their innovations and solutions, and in this way attracting investors, finding better geographical coverage and expanding besides national boundaries, as well as identifying partnerships in value networks, whether it is with larger cybersecurity suppliers or with others start-ups or SMEs that complements their solutions.

In this line, SPARTA and CONCORDIA pilot projects already started joint activities in May 2021, with the objective to find the best way to use community for the exploitation related activities. This initially included joint catalogue of existing assets from both projects, especially those depending on “community” or “network” effect, cross-pilot demos of the most relevant assets, defining role of community in the uptake or sustainability processes, as well as the role of community as a possible “validator” of deep tech start-up ideas.

The challenge here is to be able to implement assessment of highly innovative ideas through community, especially for so called “deep tech” start-ups, without disclosure of the idea itself. SPARTA and CONCORDIA exploitation managers agreed about joint actions in this direction, and drafted suggestions or recommendations about “rules and constraints for community assessment of start-up ideas”. Service scope and function, as well as list of features and capabilities was later shared with all four pilots within the focus group on start-up and SMEs.

### **5.2.6. Economic Issues in Threat Intelligence Sharing**

This section focuses on providing an overview of the threat intelligent sharing from economic perspectives, discussing the economic issues and challenges for incentivise the direction of information sharing, while also reducing the costs of cyberattacks by using threat intelligence.

---

<sup>132</sup> <https://digital-strategy.ec.europa.eu/en/policies/pre-commercial-procurement>

### 5.2.6.1. Related Work

NIST publication [102] describes the benefits and challenges of sharing, including the trust, and introduces specific data handling considerations. Some of these benefits are difficult to measure. Shared situational awareness, for example, is an obvious benefit, as well as improved security posture, but these are not directly to translate into a measurable indicator, such as e.g. reducing the number of viable attack vectors for actors.

Game-theoretic models investigate the benefits of SIS, including the iterated prisoner's dilemma [103]. One of the benefits claimed is that CTI likely reduces information asymmetry costs that defenders or blue teams face, making it particularly relevant in the context of the detection of zero-day vulnerabilities. Information asymmetry is a concept that applies within the cybersecurity market since demand side users often have significantly less information about complex products and services than the supply side or researchers. Some of the claims they make about their products or services might be refuted by testing, benchmarking or certification, but for many on demand side it is still difficult to estimate the real value. There is also more emphasis on making a noise and "influencing" (not least through influential market analyst companies), than testing features and functionality. There are probably some studies about the impact of labeling and certification, but the economic effect of the other "support" mechanisms, especially in the context of "ecosystem", could be a topic for the roadmap.

The SAINT project proposes to analyze and identify incentives to improve levels of collaboration between cooperative and regulatory approaches to information sharing. In case of Game theoretical approaches to cyber-security information sharing, they concluded when adopting a static perspective on organizations' decisions to share sensitive information about cyber-incidents, it is optimal to avoid revealing private information. A dynamic perspective was suggested to understand how time-dependent factors can influence the cooperation equilibrium. Incentives that depend on market characteristics such as the level of competition between market players, the size of organizations and the size of companies, or spill-over effects on the demand side, are also described with few recommendations (e.g. Community-Based Model for Assessing Cyber-Security Maturity, CCSM model, also described in [104] and [105]).

Value of cybersecurity information sharing in an ecosystem is also studied in [106] [107], where value parameters include the installed base (*i.e.*, the number of end users), trusted communities, Quality of Services (QoS), Quality of Information (QoI), timeliness of information, trust on information sources, and cost. These value parameters and the value functions, in which the value parameters are integrated, are used for explaining the values generated by stakeholders in the ecosystem. System dynamics simulations were used for the evaluation of value creations and value distributions in the ecosystem. Results show that value obtained by information providers is quite low in comparison to the cybersecurity solution providers and end users. While a cybersecurity information usage fee slightly affects the values for end users, it has a significant impact for information providers, indicating potential risks of unsustainability of the cybersecurity information sharing ecosystem. Notion of Quality of Indicators (QoIn), similar to "IoC feedback" suggested by CONCORDIA participants in workshop about CTI incentives (*cf.* D3.2), was also used in [108] in order to make an assessment of the level of contribution by participants in information sharing for threat intelligence.

Another study [109] is presenting representative information sharing structures and identifies the costs of information sharing and information security borne by different parties both before and after cyber-attacks, as well as the main benefits. In regard to incentives, survey has been used in [110] to find out about organization's practices and interactions with organizations that share cybersecurity information. Characteristics that incentivize share and the barriers that discourage sharing are described. Another survey-based model is presented in [111] and is tested with an exclusive dataset collected from 262 organizations that operate in the context of critical infrastructure protection in Switzerland. Sharing is measured with a multidimensional approach (intensity, frequency) and regressed on reciprocity, value of information, institutional barriers, reputation, and trust. Results show that institutional barriers have a strong impact on decision makers in Switzerland and suggest formulation of incentive-based policies that can avoid non-cooperative and free-riding behaviors. Other surveys with large number of participants (total of 1,098 IT and IT security practitioners) are Ponemon studies [112] that have more open range of questions.

Model developed in [113] applies functional dependency network analysis to emulate attacks propagation and game theory for information sharing management. It allows testing of different sharing strategies under several network and attack settings.

HERMENEUT project [114] defines itself as a Strategic CTI, and presents high-level information on changing risks to the CISO or the management board. The intention of the project is to ease the adoption of predictive reactions and the long-term inclusion of organizations in the EU CTI-based prevention model. HERMENEUT is using the proactive risk re-assessments and refinement models based on personal CISO knowledge and dark web data.

#### **5.2.6.2. Costs of Data Sharing**

There are several categories of costs related to data sharing in general, and cybersecurity threat intelligence sharing in particular. While these can be clustered into strategic (e.g., investment decision making), tactical (e.g., selection and implementation of platform) and operational (e.g., filtering of applicable data), the following considerations are proposed:

- Costs of inbound data sharing acquired from the third party (leading to more accurate understanding of the situation), which besides integration or license costs, includes risks of extending complexity, that eventually can be modeled as a new attack vector, e.g., data poisoning.
- Costs of outbound data sharing with the third party (for example to subcontract services) include risks of exposing sensitive data or knowledge. This risk could be modeled as a monetary impact due to non-compliance or loss of sensitive data.
- Collaborative (both inbound and outbound) include risks of privacy and related monetary impacts (e.g., GDPR fines). Many CTI solutions are including integration with security technologies such as vulnerability scanners, IDS/IPS and SIEMs to protect their environments before an incident occurs. The cost of integration and membership fee for community-based sharing could also sum up.

- Cost of negative externalities, another economic term that applies to cybersecurity that happens when risks of one partner in data sharing scheme are felt by the third parties.

Cyber Threat Intelligence (CTI) cost of dedicated capability has been investigated in [115], together with the funding recommendations. In their roadmap, an estimation of a cost of at least £500,000 in delivering a basic capability for CTI over the initial 18 months was estimated, mainly for third party license costs and additional resources to be contracted. Cost of CTI differs whether it is integrated natively into security products (*i.e.*, appliances and software tools) or provided as a service and several reports or comparisons between solutions exist, for instance between Anomali, ThreatConnect, ThreatQuotient, NC4, Apvera, Wapack Labs, TruSTAR, LookingGlass and EclecticIQ.

Some of these services may have different levels of data feeds to be used in a variety of security equipment, while others offer access to analysis tools and security analyst reports, with data feeds as a separate subscription. Some have trusted community membership included. Most CTI providers assume that customers have security staff already, or even security operations centers (SOC). Since SMEs do not have the manpower another concept, SOC-as-a-Service, might be considered, with managed threat intelligence service. When customers purchase threat intelligence as a subscription to one or more data feeds, there is often complex pricing scheme with tiers (*e.g.*, for each 5000 users). The cost of a data feed subscription ranges of roughly \$1,500 to \$10,000 per month. Finally, there are also services that require customers to buy their security devices along with a threat intelligence data feed subscription. Of course, there are also providers, such as company founded by the EU-funded SISSDEN project [116] that provides data for network owners and researchers at no cost.

### 5.2.6.3. Measuring Applicability and Timeliness

Cybersecurity is difficult to measure. In the past there was too much focus on “ticking off” specific risks or vulnerabilities, in the form of security audits that were discrete in time, rather than finding if resources, procedures, people and technology are adequate or if threats are applicable for the specific organization or situation. Sharing cyber threat intelligence between organizations is supposed to change this, but its benefits are even more difficult to measure because of this “applicability” factor. We focus only on operational data sharing, so time frame is very limited, and details of attacks need to be very specific.

It has been widely acknowledged that organizations can learn from each other, detect tactics or threats without having to experience these in their own systems. In theory, broader sharing of attack patterns contributes to defense against threat actors, therefore also reducing the actual attack probability. But in practice, what are the parameters that impact the benefits of sharing? More entities that participate in that scheme? Number of entities with similar threat context? Data timeliness, completeness, or accuracy?

A 2019 study by McKinsey Consulting found that risk-based vulnerability management reduces risk [117], up to a reduction of 7.5 times above the original security program, with almost no added cost. Gartner's research study found similar conclusions, stating that by adopting risk-based vulnerability management, an organization is likely to suffer 80% fewer data breaches [118]. In the same way that CVSS is a completely ineffective method for prioritizing remediation efforts since most scores employ only a theoretical view of the risk,

rather than actual risk, we can argue that threat intelligence sharing is completely ineffective if there is connection to actual risk or “applicability” measure.

In the first set of interviews with financial stakeholders, within the scope of T2.2 of CONCORDIA, we were told that it is difficult to separate the benefits of different layers of security controls. It is, however, possible sometimes to say that an incident has been detected thanks to threat intelligence sharing, and/or that time to identify and resolve it is reduced. Depending on the type of threats this can be measured in days (e.g., in case of malware) or hours (e.g., phishing). There is publicly available data<sup>133</sup> with estimates on how much it takes to respond to an incident. Besides the reduction of response time that oscillates between 60% and 80%, depending on the threat and on the entity, we also need to consider that the amount of damage that an attack cause is much higher in the first hours, and then it drops as time elapses.

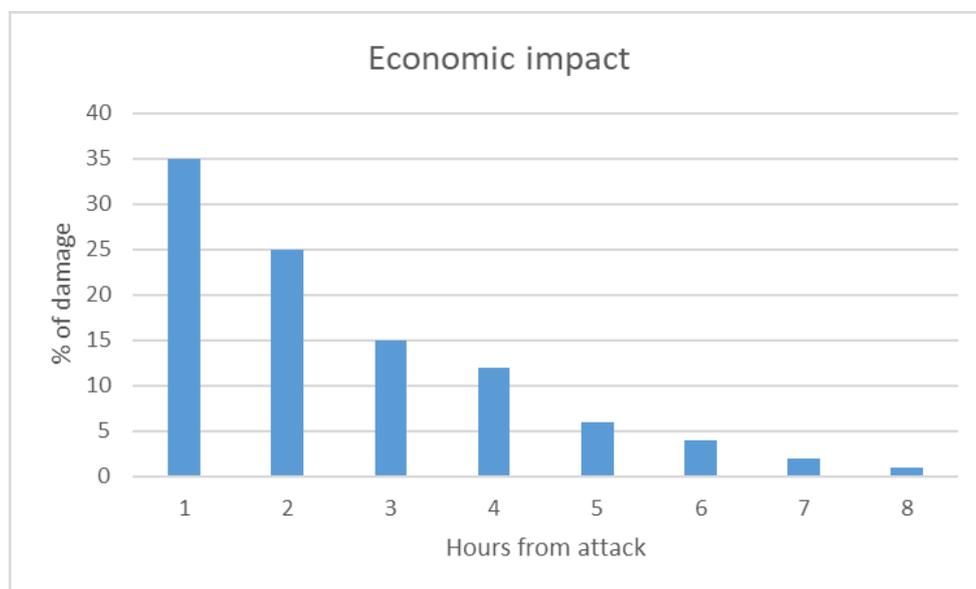


Figure 10: Estimation of Economic Impact of Phishing as Time Elapses

After this initial meeting with financial stakeholders, we decided to focus on one specific benefit of F-CTI related to phishing. The number of phishing attacks observed by APWG and its members [119] grew through 2020, doubling over the course of the year. Number of unique phishing Web sites detected, for which threat intelligence sharing is particularly helpful, was oscillating around 200.000 per month. Domains, for example, are tagged as malicious if its use for phishing was reported, for example if it contained a brand name or misleading string. The time between this first “tagging” and sharing information through CTI is very short and in the most cases less than a week. While there might be case of domains that existed for long before they were (mis-)used, it was estimated that 75% of these “phishing” domains would be identified as malicious in less than 1 week, after their activation, and that this data would be shared through different channels or in different communities.

Starting from the risk-based definition of “applicability” and cybersecurity threat intelligence definition of “actionable data” (complete, timely, accurate, relevant, and trustworthy), it was tried to measure how “timeliness” of F-CTI sharing, changes the

<sup>133</sup> <http://www.apwg.org>

perspective of the economic impact of an attack in an organization. For this analysis we used again historic data from APWG about “time to publish” intelligence concerning new malicious phishing threats, the average speed of spreading this threat intelligence data, and a “speed of digestion”, which is about converting this piece of data into “actionable” intelligence in specific organizations, in our case financial institutions.

Figure 11 shows the results of simulation of sharing threat intelligence related to a previously unknown phishing attack. For the situation when threat data is shared only one hour before the attack occurs, which implies that it might not be fully actionable or that all response measures are still not in place, we still find reduction of damage between 7% and 10%. However, in the case that information is shared > 40 hours before attack on a financial entity occurs, which is a much more likely situation, damage reduces significantly, almost to 85% of what would have been the size of damage initially, without use of threat intelligence.

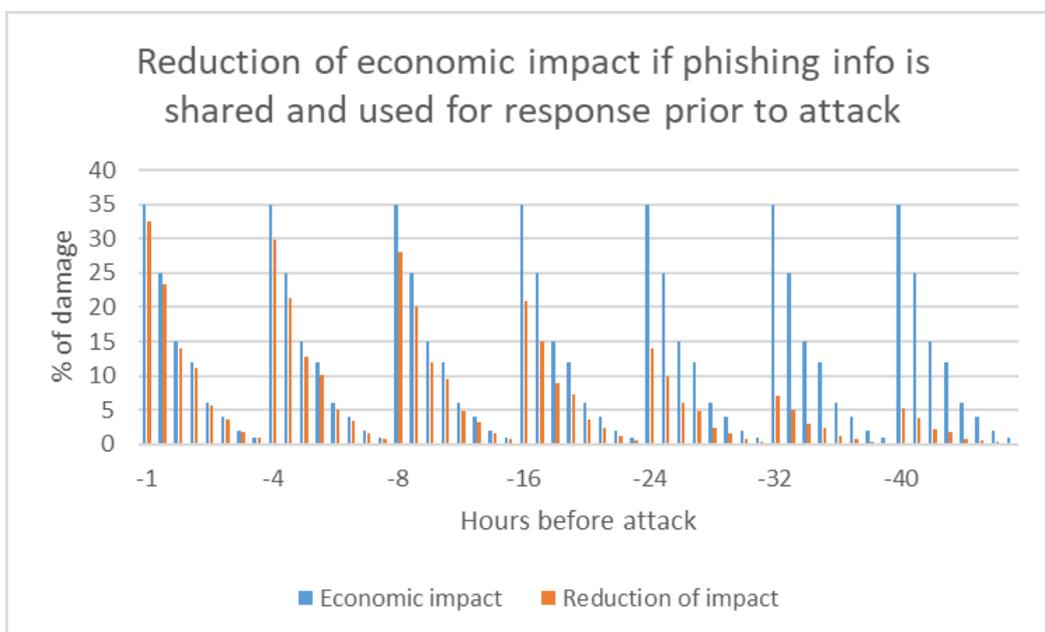


Figure 11: Reduction of Economic Impact due to Threat Intelligence Sharing about Phishing and Effect of Timeliness

#### 5.2.6.4. Other Possible Benefits and Future Research

Improving the estimation of risk probability is another benefit that happens when correlating data from CTI with, e.g., vulnerability database or data from SIEM used in real-time risk assessment engine (RAE), described in D4.2. Correcting biases in risk management is an important challenge, since risk analysts focus too much on consequences and not on probability. Systematic bias can be eliminated if continuous updates are used, while too much focus on cost/benefits of decisions only to internal assets can be reduced by including risk assessment of external risk. There is also an overlap of these risk assessment benefits with agility. Actors continually adapt their TTPs to try to evade detection, circumvent security controls, and exploit new vulnerabilities, so if we can measure agility (e.g., time to

respond to a new threat) we could also measure the supposed benefits of CTI, although it is always difficult to attribute changes to isolated factors such as use or not of CTI data. We plan to continue this work in the final year of the project. In addition, we will also analyse the economic impact of CTI data beyond timeliness, e.g., data quantity, accuracy, and completeness.

Table 5 presents an illustrative example of a qualitative approach that we plan to test during the online workshop with financial stakeholders. Values from this table are based on small number of opinions and will be enhanced with the results of a larger survey.

Table 5: Qualitative Estimation of Importance of Different Properties of CTI Data

Type of CTI Source	Internal	External Structured	External Unstructured
<b>Examples</b>	<b>Parsing data from firewall, SIEM, IDS/IPS</b>	<b>Vulnerability databases, IP black&amp;whitelist</b>	<b>NLP and crawlers processing text from darkweb, forums, social networks, news</b>
Completeness	3	3	2
Timeliness (window of reaction)	5	4	2
Timeliness (zero day)	2	3	4
Accuracy	4	4	2
Relevance	5	2	2
Trustworthiness	5	5	2

In addition, on November 17<sup>th</sup> Atos and UZH had a conference call meeting in which CERCA (Cyber Risk Calculator) demo was presented. This tool was developed by Atos and took into account some work from the previous year in CONCORDIA, in the scope of real-time risk assessment activity.

The tool receives input data from a variety of sources that can inform about changes in the target system (e.g., new threats, new target nodes, new vulnerabilities, alarms from SIEM or IDS tools). Input data can also come from historic events or questionnaires (filled by end-users), but the strength is usage of real-time indicators, such as security events/alarms, configuration changes, vulnerabilities (detected by monitoring tools), and potential threats/attack patterns (predicted by AI-based tools or provided by threat intelligence sharing). Therefore, timeliness is the most important economic impact reduction parameter.

Once a change in the risk indicators is detected, the risk indicator module will subsequently activate a risk model to be further re-evaluated. These models evaluate a series of conditions (a series of indicators) that apply to confidentiality, integrity, and availability impact to compute qualitative and qualitative risk levels. Tool demo was focused on indicators related to security incidents (e.g., events, alerts, alarms), detected by monitoring tools such as SIEM, but CTI tools could help with risk indicator design for potential threats or attacks identified by prediction models and algorithms. Considering for instance a risk model that evaluates a Distributed Denial of Service (DDoS), potential threat information includes IoC, abnormal network connections, unusual traffic loads.

Atos also presented quantitative risk assessments (e.g., cost overruns, resource consumption, delays). Economic impact of the risk is based on the impact values of Confidentiality (r1), Integrity (r2) and Availability (r3) and is expressed in monetary values (e.g., EUR). If the indicator “n” is considered coming from threat intelligence e.g. the number of IoC about phishing, the likelihood and impact values will change in function of “n”: `ifelse (n == 0, L_r <- range(0,10), ifelse(n <= 5, L_r <- range(10,30), L_r <- range(30,100)))`. In the last year of CONCORDIA, the plan is to further explore the applicability of indicators coming from CTI, as well as explore the possibility to link the output of CERCA tool with Decision support tools from UZH.

### **5.3. Kirti: Decentralized Reputation and SLA Enforcement for Cybersecurity**

Trust management in distributed systems has always been a topic of active interest in the research community to understand how to foster and manage trust aspects. In this sense, Distributed Ledger Technologies (DLT) and BC emerge as an alternative for shifting trust assumptions between users to the protocol that regulates the interaction, fostering trust in distributed systems. Especially, reputation management systems have enabled several applications to be revisited as applications running based on an underlying distributed system. Thus, a clear understanding of major properties, threats and vulnerabilities, and challenges of reputation systems based on different types of DLTs and BCs (*i.e.*, permissioned and permissionless [120]) is key to determine their usefulness and optimization potentials. In this sense, a use case of a BC-based reputation system within the context of the cybersecurity market illustrates such benefits and drawbacks of exploiting DLTs for reputation systems.

In order to address the challenge of trustworthy reputations and SLA agreements for cybersecurity providers, the Kirti platform is proposed. The work focuses on the design and prototypical development of a BC-based reputation system for the cybersecurity market, including automated SLA enforcement. In order to provide a full-fledged platform, a basic marketplace is also developed and integrated, which allows service providers to upload protection services and customers to buy and rate said services. The underlying reputation system was designed under the consideration of different attack vectors regarding rating fraud. The SLA details of all services uploaded by providers are automatically encoded into SCs, which handle the underlying protection service's payment, compensation, and termination. Furthermore, the system allows the integration with external parties, such as the recommendation system implemented by MENTOR [88], by exposing reputation data via a RESTful API. Additionally, a case study is provided to show evidence of the feasibility of the platform in real-world settings.

### 5.3.1. Kirti's Overview

The goal of Kirti [121] is to implement a decentralized reputation system for cybersecurity providers, including the generation and enforcement of SLAs using SCs. Kirti allows the upload and purchase of cybersecurity solutions whose SLA terms are encoded into SCs running on a BC, providing automatic customer compensation in the event of agreement violations. Major events of the system, such as uploading customer reviews and checking provider reputations, are fully auditable by notarizing them in the BC and storing a reference to the BC record (*i.e.*, transaction hash). Kirti's reputation system is designed with possible attacks such as *Ballot Stuffing* and *Bad Mouthing* in mind, following a decentralized approach. Additionally, its reputation data is available to external parties via a provided RESTful API. Figure 12 introduces the conceptual architecture of Kirti and describes its main components, showing the main functionalities and actors supported by the solution.

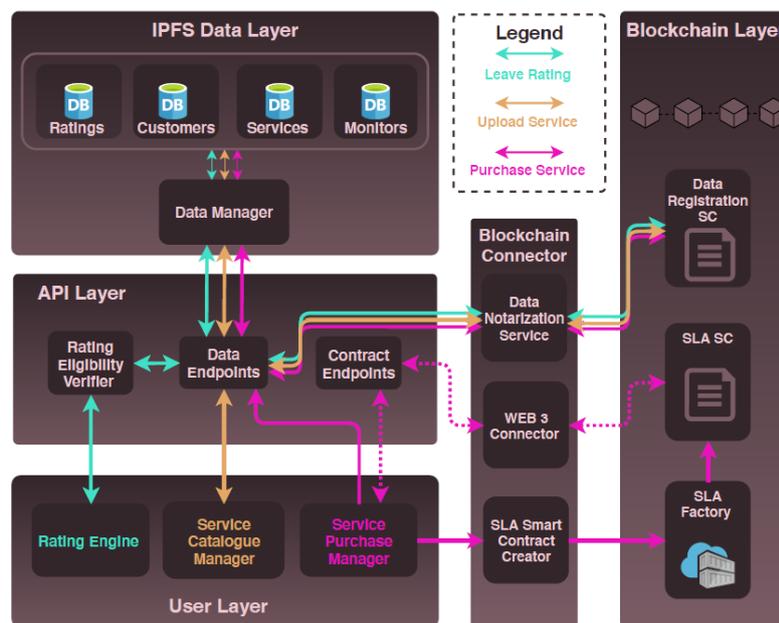


Figure 12: Kirti's Architecture

The User Layer provides a front-end, allowing users to interact with the system. Users can be divided into two groups: Those selling and those buying protection services, here referred to as service providers and customers, respectively. The Service Catalogue Manager displays the currently available services in the system and provides SPs with an interface to list a protection service up for sale. The Service Purchase Manager enables a customer of Kirti to purchase a protection service and informs him about the current state of his purchased SLAs. This information includes the current violation count as well as the time until the SLA expires. *Figure 13* depicts a summary of an example of an SLA defined and listed using the Kirti's web-based interface.

In the endeavour to design Kirti in a decentralized manner, an appropriate data storage mechanism had to be identified. The storage of data in the BC seems initially a possible approach. However, the associated costs are prohibitive. All computations on Ethereum have an associated operational cost measured in terms of *gas*. The price for a *gas* unit is termed as *gasPrice* and most commonly specified in units of Wei, where  $10^{18}$  Wei equals one Ether. A storage operation of 256 bits carries a computational cost of 20'000 *gas*. Storing

one kilobyte of data at a *gasPrice* of 50 GWei amounts to a fee of € 12.5 at a price of € 400 per Ether. Therefore, storing data on the blockchain is very expensive.

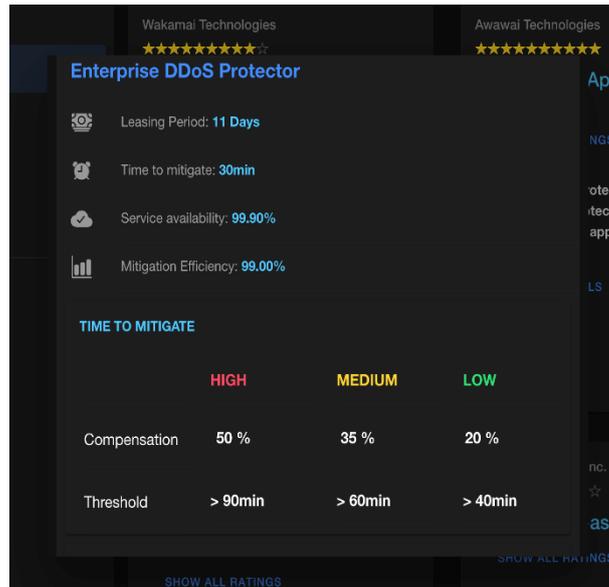


Figure 13: SLA of a Protection Contracted using the Kirti Approach

Thus, the InterPlanetary File System (IPFS) emerges as a feasible alternative to circumvent the data storage problem that BC developers face because regardless of the size of the uploaded content on IPFS, the cryptographic algorithm SHA-256, most commonly employed in IPFS, always returns a hash of 32 bytes. Hence, the data storage overhead can be effectively reduced by uploading data to IPFS and then storing only the associated 32 byte-hash in the BC.

From the external communication perspective, Kirti was designed to make reputation data available for external parties such as MENTOR [88] via a RESTful API. However, the data retrieval is slow using a BC, which makes the approach unsuitable. OrbitDB was chosen as the storage medium of choice as it harnesses the power of decentralized storage while allowing for quick data access. In an endeavour to maximize data verifiability in Kirti, each major event triggered by a customer is first recorded in the BC before being stored in the data layer. The service upload by a service provider, rating generation by a user, and an SLA contract creation are all handled similarly. In this way, audibility and transparency are ensured. Each customer rating includes the transaction hash of the transaction triggered by the Data Registration SC. Assuming a production deployment to the Ethereum main net, each rating could be audited by verifying the transaction details via the transaction hash.

The Kirti platform was implemented using different technologies. The front-end was implemented using the Ionic Angular mainly because of its support of Typescript. Ethereum was used as the BC platform and Solidity as the SC language. For the IPFS layer, the OrbitDB was used. The source code and all documentation required to run the Kirti are publicly available<sup>134</sup>.

<sup>134</sup> <https://gitlab.ifl.uzh.ch/franco/kirti>

### 5.3.2. Case Study: Usage of Kirti in the Cybersecurity Market

This case study focuses on the different features of Kirti to showcase the functionality of the system in a real-world setting. A user of Kirti is either a service provider, a customer, a monitor, or an external party interested in the reputation data of cybersecurity services. To begin with, the owner of the monitoring solution *ArgusEyed* is interested in acting as a monitoring solution for Kirti. The owner then makes a POST request to the end-point of its RESTful API as exemplified in Listing 2. Upon successfully registering the details in the IPFS Data Layer, the owner is thus informed and may now be selected as the monitoring solution for a deployed protection service.

```

1 {
2   "name": "ArgusEyed",
3   "address": "0 x9d8d840d00aa17e3f9adf03421a2b4dd43d06c3c "
4 }

```

Listing 2: Body of the Request Sent to the End-Point /orbitdb/monitors/add

Next, assume the provider Piranha Networks, Inc. wants to make his/her protection service Piranha Web Application Firewall (WAF)-as-a-Service available to customers via Kirti. Thus, he/she navigates to the appropriate section in the front end to enter his service's general details as well as its SLA specification, which takes no more than two minutes. Upon confirming the service upload, the provider is informed by a popup that his service upload was successful and is displayed the hash of the transaction which registered his service upload with *registerService()* of *Kirti.sol*, namely *0xccca4...eff56b7*.

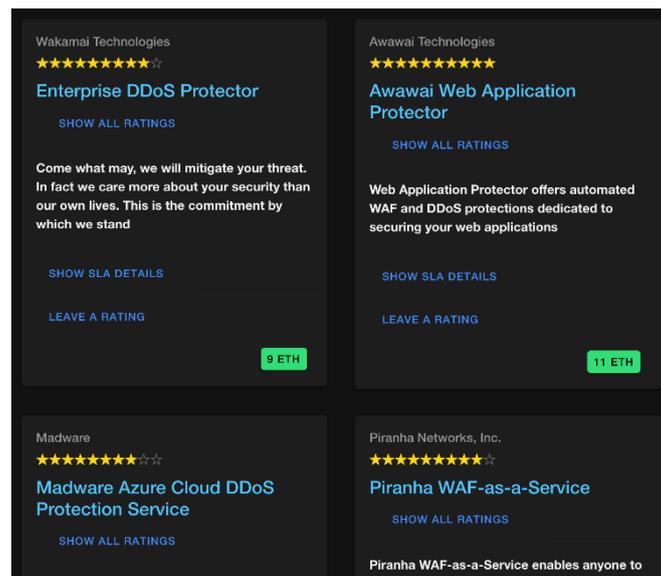


Figure 14: Kirti's Marketplace

Now let supposing that a specific customer is interested in purchasing a WAF to secure his/her web application. He/She thus navigate to the overview of available protection services in the front-end, as shown in Figure 14. After a short inspection and comparison of a potential solution, he/she opts to purchase Piranha WAF-as-a-Service as the service that matches his/her technical requirements, as it offers a generous SLA compensation, and is well rated by fellow customers. The fact that he/she can verify each review on the Ethereum BC further increases his/her trust in the validity of customer ratings. After confirming the purchase, the front-end displays a popup asking the customer to select a monitoring service

in charge of surveilling the protection service and reporting violations to the SLA SC. After selecting *ArgusEyed* as the monitor, a popup shows that an SLA SC as encoded by *SLA.sol* has been deployed at address *0x545d8...4D91FCAC*. Next, MetaMask (a BC wallet plugin) pops up, with the transaction details regarding the newly created contract's address and its price already filled out. The user now has to confirm the transaction.

If the transaction was successful, the user is informed and may also verify the transaction details. The user may now navigate to the My Services section of the Kirti's dashboard to inspect the current state of his/her newly purchased service, as demonstrated in Figure 15. Of particular importance is the Current Compensation field, which displays the up-to-date value of the SLA's compensation as calculated by the number and severity of reported violations.

Now that the SLA SC is activated through the user's payment, the monitor must check the deployed protection service. Suppose now that a DDoS attack on the customer's web application takes place. Luckily Piranha WAF-as-a-Service includes DDoS protection. While the attack is successfully mitigated, the monitor notices that the mitigation took 62 minutes instead of the promised 30 minutes as specified in the SLA agreement.

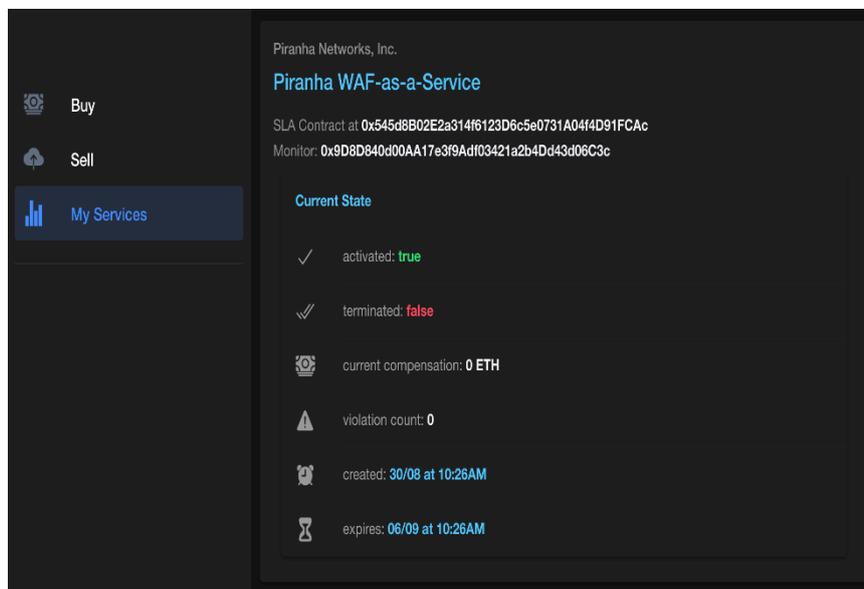


Figure 15: State of a User's Services

The monitor may now call the */contracts/0x545d8...4D91FCAC/thresholds* endpoint to receive information about the SLA's threshold values regarding the violation severities. Using the obtained data, he/she concludes that he/she should report a violation of the severity medium of the Time to Mitigate metric. Note that to make a successful request to *contracts/:address/violation*, a monitor must include a message and signature to verify his identity. The monitor then generates a unique message and signature using Ethereum's Elliptic Curve Digital Signature Algorithm (ECDSA).

```

2 "message": " b9f9e1ee -55e9 -4 df7 -a83a - d5156813e192 ",
3 "signature": "0 x4184f ...24 fef00 ",
4 "violationType": 0,
5 "violationSeverity": 1
6 }

```

Listing 3: Truncated Request Body to /contracts/:address/violation, Reporting a Medium Severity Violation of the Metric “Time to Mitigate”.

The monitor now sends an HTTP POST request to /contracts/:address/violation, including the obtained values for message and signature, as presented in Listing 3. Note that the values of 0 for *violationType* and 1 for *violationSeverity* correspond to Time to Mitigate and medium, respectively. A monitor is informed about the encoding scheme regarding both *violationType* and *violationSeverity* in the response body of a call to /orbitdb/monitors/add. Meanwhile, the customer sees in the front-end that a violation has occurred, and the current compensation has been updated to an amount of 2.45 Ether (*i.e.*, 35% compensation at a price of 7 Ether). After seven days, the service and its associated SLA SC expires, the contract terminates by refunding 2.45 Ether to the customer and releases the remaining funds to the provider.

Finally, after the contract is finished, the user can provide feedback in form of a rating. For that, the user can evaluate the different dimensions of the services, such as features, price, usability, the accuracy of the promised protection, and the support received from the provider. Figure 16 shows an example of the interface provided by Kirti for the rating process.

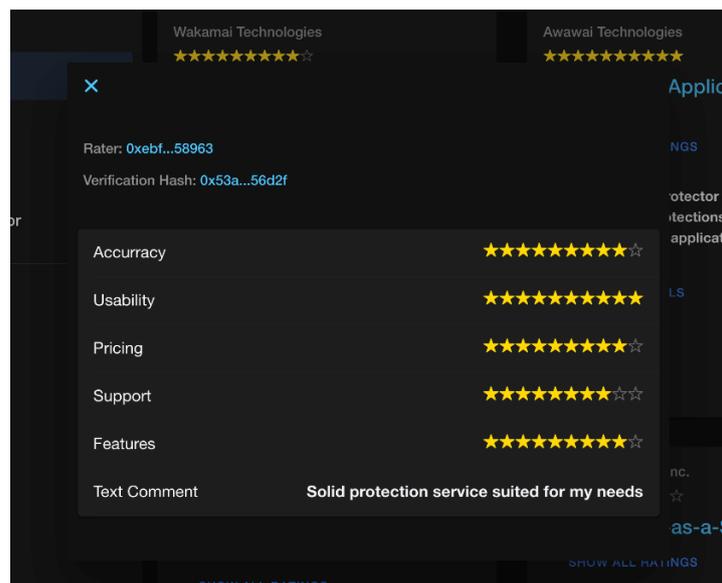


Figure 16: Rating of Service using the Kirti's Interface

### 5.3.3. Discussions on Costs, Decentralization, and Rating Fraud

For the interaction with the Kirti's SCs, first, they have to be deployed to one of the Ethereum networks, which runs them on Ethereum Virtual Machines (VM). Executing operations on the Ethereum VM is associated with costs measured in gas which carry an associated gas price in Ether. Thus, deploying and interacting with Ethereum SCs is associated with real-world costs, which were analyzed for the setting of Kirti.

Of the two SCs implemented, *Kirti.sol* has to be deployed only once while a new instance of *SLA.sol* has to be deployed for each purchased service. The deployment of *Kirti.sol* is associated with a cost of 3'383'264 gas, while the deployment of *SLA.sol* amounts to a cost of 2'397'165 gas. The *gas* costs of the publicly callable functions of *SLA.sol* are shown in Table 6. The specification of equivalent at currency values has been purposefully omitted due to the extreme fluctuations of *gas* prices. Note that at the start of the Kirti development (March 15th, 2020), Ether was priced at € 111, and the average *gas* price was around 17 GWei. Six months later (September 2020), Ether was valued at € 435, while average *gas* prices have spiked to 236 GWei. Thus, executing any operation on the Ethereum network, such as a contract deployment, has become more expensive by a factor of 50 over less than half a year. It should be pointed out that both SCs were not implemented to be maximally deployment cost-efficient. As such, SCs providing similar functionality could be significantly more cost-efficient. However, Kirti's design would remain the same.

Table 6: Publicly Invocable Functions of the Kirti's SLA.sol Sorted by Gas Cost

SC Function	Number of Calls	Gas Cost
init()	Once	473717
initOraclizeCallback()	Once	123659
reportViolationFromAPI()	0...n times	116283
payForService()	Once	86852
getState()	1...n times	29599
getValidityPeriod()	1...n times	25815
updateCompensation()	1...n times	24471
getViolations()	1...n times	23693
terminate()	once	16352

Kirti has been designed in a decentralized manner, and while it combines distributed technologies such as the Ethereum BC and IPFS, certain limitations concerning true decentralization arise. While Kirti's architecture can be deemed decentralized, in its current form, it can only be operated in a politically centralized manner, *i.e.*, by a single operator acting as the system's owner. This limitation arises due to various technicalities of its implementation. As such, functions of the SC, which records major events of the system in the BC and handles the creation of new SLA SCs, are only callable by the contract owner. Along the same lines, some of the API Layer's endpoints are required to be only accessible to the entity which owns the system. In the current state of Kirti, the system's owner pays for the deployment of SLA contracts, but deployment fees could trivially be allocated to customers and/or providers.

Besides these two types of actors, external monitors play an integral part of Kirti, as they are in charge of reporting violations to SLA terms. It is essential that these monitors can be trusted to report violations correctly, implying that they must be capable of adequately surveilling protection services. This presents a challenge to the *status quo* of the cybersecurity market and raises the question of the availability of solution providers who would act as monitoring solutions in a setting similar to Kirti's. Currently, there exists no compensation scheme for monitoring solutions. Nevertheless, it seems reasonable to remunerate monitors according to a proportionate amount of the total service cost.

It should be mentioned that any reputation system which is based on subjective measures, such as user ratings, cannot fully mitigate the attacks of *Bad Mouthing* and *Ballot Stuffing*. There is, by definition, no way to quantify the correctness of a very personal sentiment

objectively. However, by ensuring that only verified customers are entitled to leave ratings, a reputation system can increase its resilience against rating fraud. Rater verification protects against *Bad Mouthing* since the benefit incurred by rating a competitor's service negatively is likely outweighed by the cost of having to purchase said competitor's service as the best option.

Additionally, Kirti ensures that a customer may only leave a single rating for each time he/she purchased a service. Otherwise, the reputation system would be prone to rating attacks, as a customer could purchase a service only once and later on leave multiple malicious ratings. It is worth noting that rater verification is not as effective against *Ballot Stuffing* attacks. However, in Kirti, a service provider could potentially purchase his/her own service and rate it most favorably afterward. For a full decentralization, Kirti does not enforce the creation of user accounts, as such an Ethereum address is sufficient to interact with the system. This implies that the cost of creating a new identity is trivial. Thus, a malicious service provider interested in boosting his/her reputation can generate a number of different identities at a low cost.

#### **5.4. SecRiskAI: ML-based Tool for Cybersecurity Risk Assessment**

Despite the many risk assessment standards available (*e.g.*, ISO 31000, TOGAF, and NIST SP 800-30) and multi-sector assessment frameworks proposed [122], organizations still find this activity very challenging and are often confronted with a huge volume of unstructured data, which are essential for finding indicators of unpredictable risks [123]. In this case, traditional techniques are not suitable to provide valuable insights and or provide a limited ability to perform a real-time risk assessment. Hence, there is a need for continuous risk assessment and monitoring strategy for Key Risk Indicators (KRIs) in order to identify and estimate the likelihood of unpredictable threats.

Recent studies on possible applications of Artificial Intelligence (AI) and Machine Learning (ML) algorithms have highlighted their ability to process large amounts of structured/unstructured data, extract valuable patterns, learn from historically collected records and make accurate predictions. Thus, SecRiskAI is introduced to explore the potential of applying ML algorithms in the field of cybersecurity risk assessment. SecRiskAI is an approach for conducting qualitative cybersecurity risk assessment using ML techniques. In this section of the report, the SecRiskAI [124] is introduced, starting with a high-level overview of its architecture and a description of each component involved. Next, the ML-based risk assessment workflow is described, and the scope of each phase is clearly defined. Finally, details on the integration with MENTOR's recommendation API [88] is provided.

##### **5.4.1. Conceptual Architecture of SecRiskAI**

Figure 17 illustrates a high-level architecture overview and highlights the system components' interactions, with its steps being represented within red circles. In Step 1, the user is able to access the dashboard through any browser without the need for an account. The Graphical User Interface (GUI) (*i.e.*, Web-based interface) was designed in a way to provide total visibility of business-related KRIs and, at the same time, increase productivity and better forecasting of important aspects related to the business security. Moreover, through the GUI, the user is able to change both contextual information and other parameters (*e.g.*, available budget, service type and desired deployment/leasing period) required for the risk assessment and the protection service recommendations.

In order to use the information provided by the user to predict risks, an additional layer is required. In this approach, this task is performed by the Middleware (Step 2). More specifically, as soon as the request sent by the client is received, the *Request Processor* processes it and forwards the information to the *Profile Evaluator*, which is in charge of executing the ML models, evaluating the prediction response, and, when specific conditions are fulfilled, establishing a connection with MENTOR (Step 6).

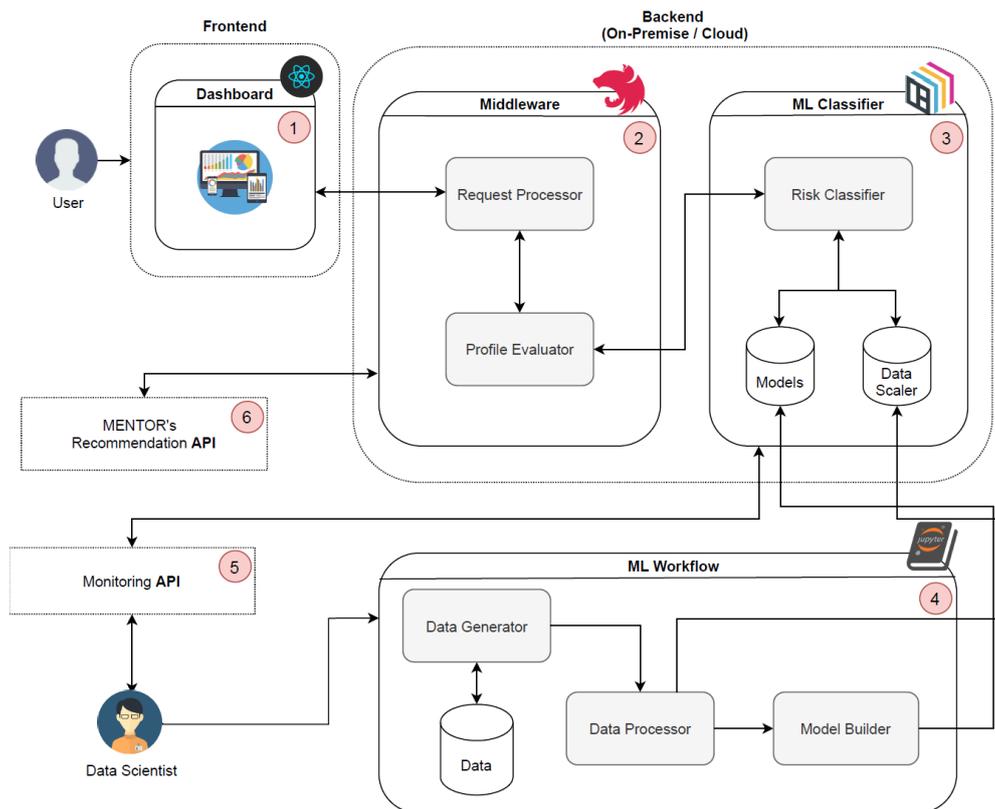


Figure 17: The SecRiskAI Architecture

To perform the actual risk prediction, a request to the *Risk Classifier* is sent. The Risk Classifier is a prediction service included in the ML Classifier Layer (Step 3) and is essentially used to expose the trained ML models through the API. Additionally, the ML Classifier Layer also stores the trained ML models as well as the *Data Scalers* used to normalize the input data and increase prediction accuracy.

The process of training, validating and testing the ML models takes place in the ML workflow Layer (Step 4) and is usually carried out by data scientists/experts in the company. In summary, the *Data Generator* component is used to initialize the synthetic data generation process. Afterwards, the data is processed (*i.e.*, Data Processor) and used by the *Model Builder* for training, validating, testing, and building the models. Each phase of the ML Workflow is described with a sufficient level of detail in Section 5.4.2. Lastly, the interface indicated by Step 5 provides a monitoring API, that can be used to check the status of the deployed models, and to retrieve model-specific metadata (*e.g.*, version, creation time, accuracy) and other metrics about the prediction service (*e.g.*, request duration in seconds).

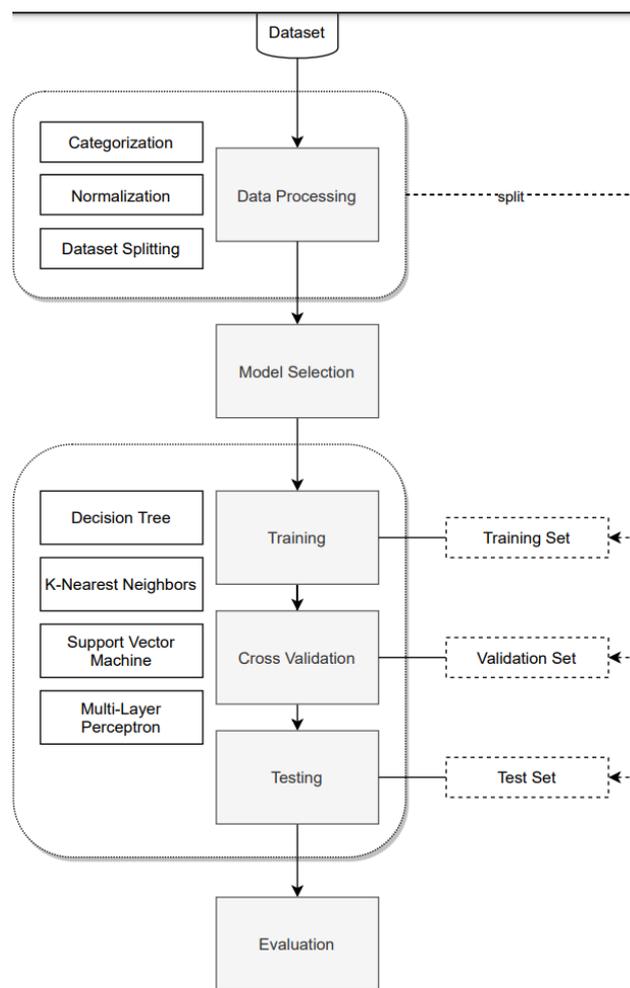


Figure 18: Supervised Learning ML Workflow Implemented by the SecRiskAI Approach

#### 5.4.2. Risk Assessment Workflow, Data Gathering, and Processing

Once the opportunities of applying ML to cybersecurity risk assessment are defined and well-understood, the process of designing and developing a ML workflow (*cf.* Figure 17-Step 4) begins. Figure 18 depicts a flowchart of the supervised ML workflow implemented by SecRiskAI, as a crucial part of the solution. After the initial problem definition, the most important stage is data collection/gathering. Usually, in this phase, data is collected from devices, sensors, or other different sources and stored for further processing. However, in the field of cybersecurity risk assessment companies either do not disclose any kind of information at all or in some cases they publish various reports which are often incomplete and difficult to extract meaningful and interesting results from. To address this issue, a synthetic data generation approach was designed and implemented.

Synthetic data is commonly referred to as data that is created by different algorithms that try to mirror the statistical properties of the original data without revealing any actual information about the subjects [125]. After exhaustive research and analysis of different cyberattacks and corresponding companies' contextual information, the following parameters used as the basis for this work were identified:

- **Revenue:** Referred to the income generated from normal business activities and operations, and, in most cases, also used to classify businesses by providing a scale for determining their sizes
- **Cybersecurity Investments:** Normally, businesses already have cybersecurity investments strategies in place to ensure a proper level of protection. This kind of information needs to be taken into consideration during the cybersecurity risk assessment, as it may have an impact on the likelihood of being targeted by a cyberattack.
- **Number of Employees and Training Level:** Similar to the revenue, information regarding the actual number of employees in a company as well as the corresponding cybersecurity training level (*e.g.*, cybersecurity basic knowledge and phishing training) represent essential contextual information required for assessing possible cyber-risks. The employee training level is measured in *Low*, *Medium*, and *High*.
- **Successful/Failed Cyberattacks:** These parameters are meant to indicate the number of cyberattacks that the company has already experienced. This includes different attacks (*e.g.*, DDoS, Ransomware, and Phishing) that have targeted the organization's infrastructure and resulted in either a financial loss or reputational damage. Failed attempts (*i.e.*, attacks that were not successful) are also taken into consideration.
- **Known Vulnerabilities:** For an effective and comprehensive risk assessment, it is essential to report any known vulnerabilities of the infrastructure. Vulnerability management is usually a key responsibility of the companies' IT security team. This phase usually involves assessing and reporting any security vulnerability present in the organization's systems [2]. There are a variety of comprehensive tools used for vulnerability scanning, such as Nmap, Metasploit, and OWASP. Currently, the total number of known vulnerabilities is defined during the synthetic generation process.
- **External Cybersecurity Advisor:** In order to further strengthen their cyber resilience (*i.e.*, the ability to prepare for, respond to, and recover from cyberattacks), businesses are encouraged to hire external Cybersecurity Advisors (CSA) [7]. Furthermore, CSAs provide a variety of services, such as cyber preparedness, strategic messaging, working group support, partnership development, cyber assessments, incident coordination and support [126]. During the synthetic data generation phase, a binary value will be generated (either *Yes* or *No*).
- **Risk:** The last parameter represents the value of the qualitative risk assessment based on the previously generated parameters. Since the synthetic data generation process is designed to generate historical records of companies operating in comparable industries, the value of the risk column may be derived from past formal or tailored qualitative risk assessment techniques. The generated risk can have one of the following values: *Low*, *Medium*, and *High*.

In order to generate the synthetic information mentioned above, assumptions were made. First, upper/lower boundaries for each column were specified, so that each generated value would effectively lie in the defined range. Table 7 presents an overview of the determined boundaries as well examples of values for each generated information.

Table 7: Overview of the Generated Data

Information	Range	Value Example	ID
Revenue	0 – 5,500,000	2,500,000	Business_value
Cybersecurity Investment	0 to 30% of the business value	500,000	Invested_amount

Successful Attacks	0 to 50	5	Succ_attack
Failed Attacks	0 to 50	12	Fail_attack
Number of Employees	30 to 10,000	4,450	Nr_employees
Employee Training	Low, Medium, or High	Medium	Employees_training
Known Vulnerabilities	0 to 10	8	Known_vul
External Cybersecurity Advisor	Yes or No	No	External_adv
Risk	Low, Medium, or High	Low	Risk

It is important to note that the risk is not randomly generated, instead, it is computed based on the generated attributes illustrated in Table 7 using the generalized formula described in Equation 4. For a supervised learning algorithm to work, the dataset must be labelled. As a result, the *computed\_risk* output is mapped to either a *Low*, *Medium* and *High* class. However, a manual labelling process would be not scalable, since the generated dataset would include thousands of records. Therefore, based on the numeric value of *computed\_risk* a mapping range was defined. This means, that each *computed\_risk* value is labelled using the range specified in Equation 4.

Once enough data has been successfully generated, the processing phase starts. The ML algorithms require additional processing steps as they are not able to work with raw data. In the first step, any categorical variable present in the dataset is handled. Specifically, variables such as *employee training level* and *external cybersecurity advisor* are mapped to numerical values, which are easier for ML algorithms to work with. A further normalization is necessary, which depends on the selected ML algorithm. Normalization is the process of scaling data into a pre-defined range (e.g., 0 to 1). Some ML algorithms (e.g., SVM and k-NN) are known to be highly sensitive to features with varying degrees of magnitude, range and units.

The dataset generated for this work includes features, such as *revenue* and *number of employees* that have different ranges, which may lead to lower performance and accuracy during the training of sensitive models with such unscaled data. In this solution, a normalization technique known as Min-Max scaling was used. The Min-Max normalization technique is applied to the entire dataset but only to *features*, namely every column except *risk*, which contains the three output classes (i.e., High, Medium, or Low) based on which future predictions will be made. The last step in the processing phase involves splitting the dataset into a training, validation, and test set, as illustrated in Figure 19.

$$i_r = \frac{invested\_amount}{business\_value}$$

$$e = \frac{nr\_employees}{tot\_empl} * map(employees\_training)$$

$$att_r = \frac{succ\_attacks}{max\_attacks}$$

$$v_r = \frac{known\_vuln}{max\_known\_vuln}$$

$$adv_i = map(external\_adv)$$

$$map(x) = \begin{cases} 0, & \text{if } x = Low \\ 1, & \text{if } x = Medium \\ 2, & \text{if } x = High \end{cases}$$

$$computed\_risk = i_r + e + adv_i - att_r - v_r$$

$$risk(x) = \begin{cases} High, & \text{for } x < 0 \\ Medium, & \text{for } 0 \leq x < 1 \\ Low, & \text{for } x \geq 1 \end{cases}$$

Equation 4: Risk Calculation Proposed in the SecRiskAI Approach

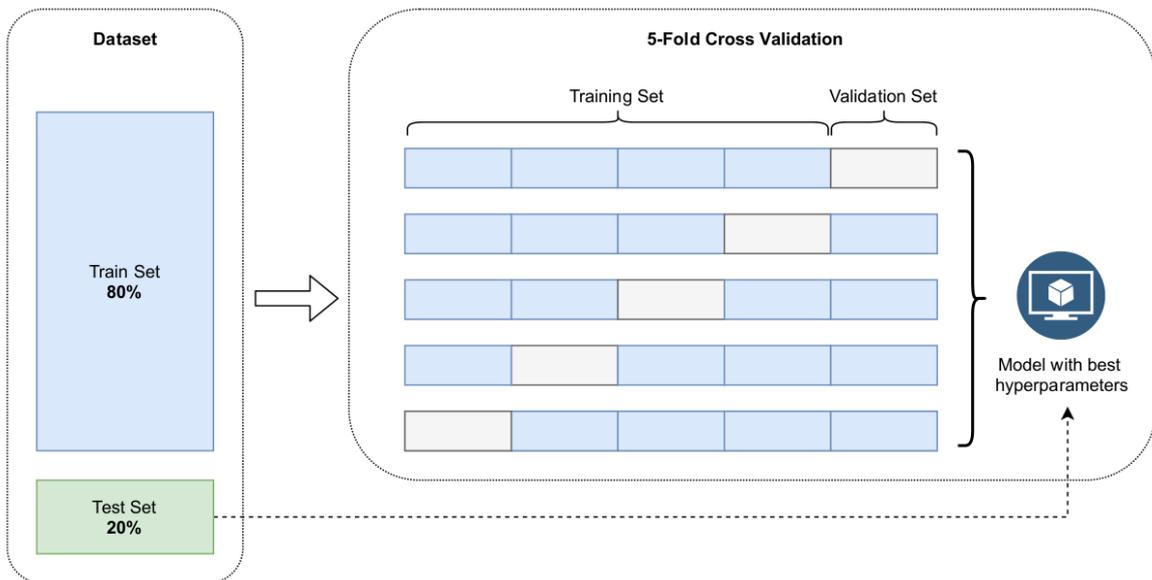


Figure 19: Training, Cross-Validation, and Testing Workflow

Once the dataset is generated and the required ML algorithms selected, the training phase is initiated (*cf.* Figure 18). First, the dataset is split following the 80-20 train-test strategy. Next, the process of choosing a set of optimal *hyperparameters*, also called *hyperparameter optimization*, takes place.

The main idea of this process is to use grid search to extensively test every combination from a pre-defined list of parameters values required by the ML algorithm for building the model. Subsequently, the performance of each model is evaluated with the help of a 5-fold Cross Validation (CV) strategy. The model with the highest accuracy is selected and tested with unseen data, *i.e.*, the test set. Lastly, the entire process is applied to each ML algorithm discussed in the previous sections.

### 5.4.3. Multi-Class ML Classification Algorithms

In ML, Multi-Class Classification (MCC) algorithms aim to solve problems of classifying instances into one of three or more output classes. In the model selection phase (*cf.* Figure 18) popular MCC algorithms are selected for conducting qualitative cybersecurity risk assessments. The main goal is to design and develop ML models that, based on actual contextual information, can make accurate qualitative risk assessment predictions and further monitor the organization's infrastructure by providing continuous assessment based on input data.

#### 5.4.3.1. Decision Tree

Decision Tree (DT) is a Supervised Learning (SL) algorithm for classification used in the proposed SecRiskAI. This technique essentially looks at the feature values of the input dataset and categorizes them according to a specific parameter, also known as information gain. In the first phase, these algorithms iterate over every feature column in the input dataset  $D$  containing the organization's historical data and they compute the information gain. The goal is to find the feature column having the highest information gain which will, in turn, serve as a decision node of the tree. Next, the algorithm continues splitting the dataset on the identified decision node and performs the same search on the sub-datasets. This way, a tree structure is constructed with each node representing a feature column and the leaves indicating the output class.

Besides being a straightforward classification technique, DT can be trained on historical data, without requiring extensive data pre-processing. That is, compared to other classification algorithms used in this approach, the DT requires less effort for data preparation and the normalization step is not required. Hence, the resulting model is easy to understand for both technical and non-technical stakeholders. Figure 20 depicts a visual representation of a DT algorithm trained on the generated dataset. In order to make a prediction using the DT, a sample  $i$  would traverse the tree based on each feature value and the resulting leaf value would be the output class.

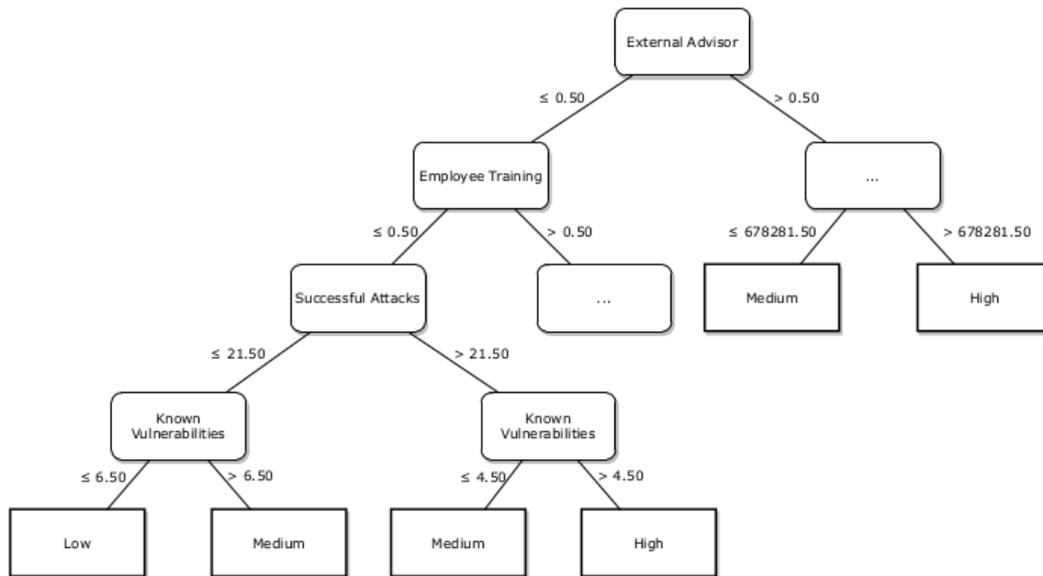


Figure 20: Visual Representation of the SecRiskAI DT

#### 5.4.3.2. K-Nearest Neighbour (KNN)

K-Nearest Neighbours (KNN) is another SL algorithm used to solve classification problems. More specifically, KNN is usually referred to as instance-based classifier as the main idea behind this technique is to memorize the input dataset to make future predictions. KNN requires three input parameters: a dataset  $D$  containing the historical information is given, a chosen number of neighbour's  $k$  and  $x$ , a sample that is to be classified. The algorithm then proceeds on computing the distance between  $x$  and every record contained in  $D$ . Next, the computed distances are sorted in ascending order and  $k$  closest samples, also known as neighbours, to  $x$  are selected. Finally, the predicted class of  $x$  is based on the similarity with the neighbours, meaning that  $x$  is labelled following a majority voting of classes among the neighbours.

In essence, KNN calculates the probability of a sample  $x$  belonging to a specific class, based on neighbour's observations. On one hand, compared to the DT, KNN requires more data pre-processing. On the other hand, the training phase is definitely faster and new training data can be seamlessly added without the need of reconstructing the model. In Figure 21, a visual representation of the KNN classification with  $k$  equal to seven and  $x$  being a new sample to classify is depicted. In this example, only two dimensions are taken into account (*i.e.*, cybersecurity investment(s) and number of employees). Once the  $k$  closest neighbours to  $x$  are identified, it is apparent from Figure 21 that the predicted class of  $x$  is *Low*, since the majority of the neighbours belong to the *Low* class.

#### 5.4.3.3. Support Vector Machine (SVM)

The Support Vector Machine (SVM) is the third SL classification algorithm considered in this work. In contrast with DT and KNN, SVM uses a line or hyperplane to separate input data into classes. Moreover, SVM is known to be computationally less expensive than KNN but does not support MCC natively. To achieve that, a *One-vs-Rest* strategy is followed. First, the multi-class dataset is broken down into multiple binary classification problems, as highlighted in Figure 22. In this case, the following classification problems are identified:

(1) High vs {Low, Medium}, (2) Medium vs {Low, High}, and (3) Low vs {Medium, High}.

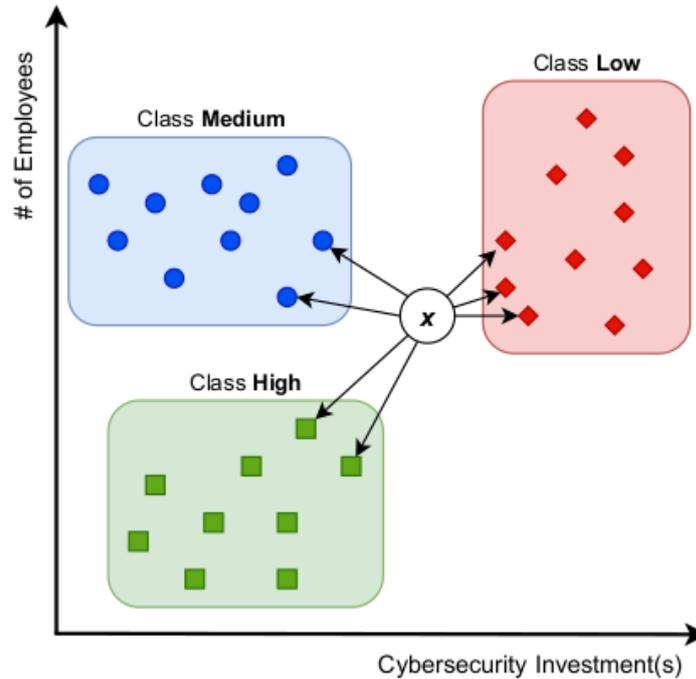


Figure 21: Visualization of the KNN Algorithm

Next, a binary classifier is trained on each binary classification problem and is able to predict a class probability ( $P_{\text{class}}$ ), *i.e.*, the probability of an object belonging to a specific class. After the training phase, the binary classifiers return the probability of a sample being labelled as *Low* ( $P_{\text{Low}}$ ), *Medium* ( $P_{\text{Medium}}$ ), and *High* ( $P_{\text{High}}$ ). Finally, the model that is able to predict the class of an unclassified sample  $x$  with the highest confidence is selected and is represented with the Equation 5:

$$\text{Class}_x = \text{argmax}(P_{\text{Low}}, P_{\text{Medium}}, P_{\text{High}})$$

Equation 5: Prediction of the Class with Highest Confidence

When dealing with larger datasets and  $n$  output classes, SVM would require the creation of  $n$  binary classifiers for each class, resulting in high computational costs. Further, SVM does suffer from performance issues when confronted with overlapping classes, *i.e.*, data points being not well separated. However, SVM is a very flexible algorithm and allows the specification of a *kernel* function that can be linear (*cf.* Figure 22) but can also be of different types, such as nonlinear, polynomial, radial basis function, and sigmoid to solve several non-linear problems.

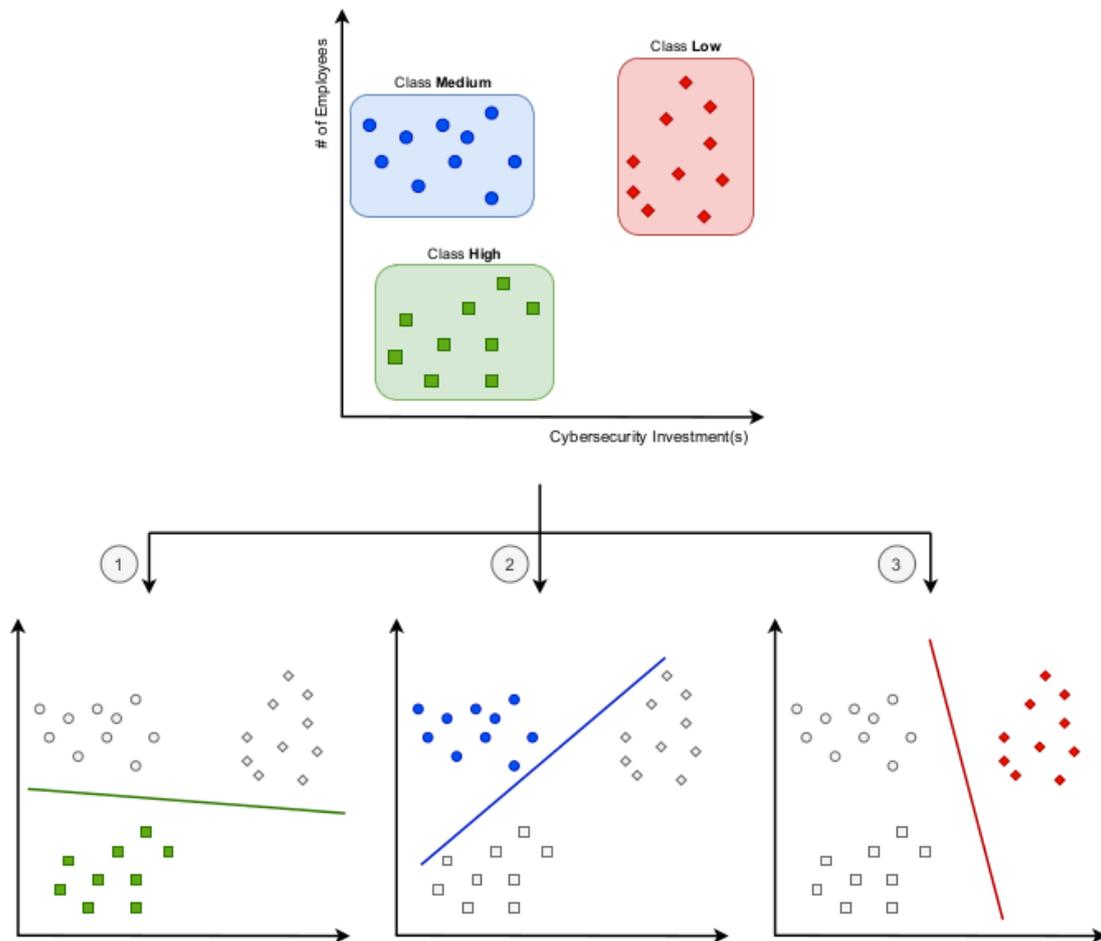


Figure 22: Visualization of the SVM Algorithm

#### 5.4.3.4. Multi-Layer Perceptron (MLP)

Multi-Layer Perceptron (MLP) is the fourth and last SL classification algorithm explored in this work. More specifically, MLP is a class of feedforward Artificial Neural Network (ANN); hence, it inherits the characteristics of ANNs, such as input layer, hidden layer(s), output layer, *perceptrons* and activation functions. Figure 23 depicts a simplified visual representation of the MLP model constructed for SecRiskAI. Each node in the input layer corresponds to a specific feature of the generated dataset. Moreover, as highlighted in yellow in Figure 23, the MLP model has a total number of two hidden layers having five neurons each.

However, choosing the best parameters for an ANN is a very challenging task, as there are no clear rules and it depends on the complexity of the underlying problem. For this work, the decision was based on the guidelines proposed by [127] as well as extensive exploratory research and testing. Nevertheless, the output layer was defined based on the output classes of the model (*i.e.*, Low, Medium, and High). Therefore, it consists of three neurons representing each possible classification state.

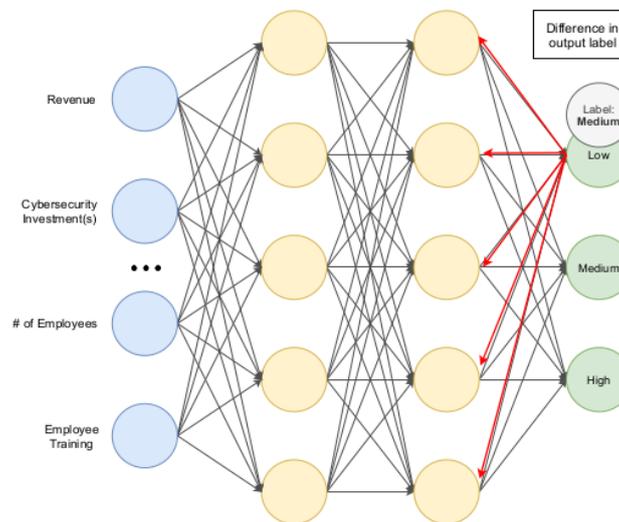


Figure 23: Visualization of the MLP Algorithm applied in SecRiskAI

During the training phase, the MLP uses a technique called *backpropagation*. An ANN propagates the input data forward through the neurons towards the output layer, where the prediction occurs. The *backpropagation* algorithm refers to the process of propagating the information about the prediction error backward from the output layer throughout the entire network with the goal of adjusting weights and improving accuracy. Figure 23 highlights in red arrows an example of a *backpropagation* mechanism initiated as soon as the original label (Medium) and predicted class (Low) differ. The computed error/loss is defined by the simplified difference between the actual and predicted output. Lastly, such *backpropagation* algorithm is used to adjust the weights in the hidden layers.

#### 5.4.4. MENTOR'S API Integration

MENTOR [88] is a protection service recommender system proposed in the context of the CONCORDIA project (and reported in the Deliverable D4.2) aiming to support the cybersecurity detection/mitigation decision process. More specifically, the MENTOR system implements four different similarity measurements to recommend the adequate protection service based on customers' profiles and needs. A typical customer profile required by MENTOR would contain the following information: (a) the region where the company operates, (b) deployment time and leasing period of the service, and (c) pricing. Moreover, MENTOR offers the possibility to filter out further services based on type (*i.e.*, Reactive/Proactive) and the specific attack type covered by the service [128]. In addition, customers can arbitrarily assign priorities for some attributes in order to receive a more tailored recommendation.

Additionally, new protection services are automatically being added to MENTOR from Protection Service Providers (PSPs) through a dedicated API. The recommendation engine can also be extended with other similarity measures and is designed to be loosely coupled from the other components in the system. Most importantly, MENTOR offers an API that, based on the customer's profile (specified as JSON), returns a list of recommended services.

To exploit such a functionality, SecRiskAI is designed to integrate the functionality of MENTOR to fully support the customer through the entire risk assessment and cybersecurity investments decision process. More specifically, the Middleware layer (*cf.* Figure 17 - Step 2), based on the data collected by the user and the cyber risk prediction, is

in charge of retrieving the list of recommended protections. Finally, this information is used to provide, in the Web-based interface of SecRiskAI, the most suitable protection services against the previously identified and assessed threats.

#### 5.4.5. Discussion and Limitations

The implemented proof-of-concept is publicly available<sup>135</sup>. It can assess the risk only for a sub-set of well-known cyber-attacks, namely DDoS and Phishing. For that, the prototype requires a specific set of attributes, also referred to as the profile or contextual information. Based on this type of data, SecRiskAI is able to predict the likelihood of a company being targeted by either DDoS or phishing attacks. Besides that, the current prototype also supports the integration with MENTOR to provide a list of recommended protection services based on the profile and influenced by the calculated cyber-risk. Additionally, the integration with MENTOR was designed to be fully configurable, meaning that the user is able at any point to update and set the priority to different profile attributes; thus, triggering a new recommendation process.

As mentioned above, SecRiskAI provides a user-friendly and intuitive dashboard design along with a valuable and accurate cybersecurity risk assessment for DDoS and phishing attacks while being integrated to MENTOR, a tool for cybersecurity protection service recommender system. Case studies were described to analyse and investigate various aspects and functionalities currently offered by the SecRiskAI prototype [129]. Furthermore, a quantitative evaluation of the various ML algorithms was performed to demonstrate that for larger datasets, SVMs achieve slightly higher accuracy, while maintaining a lower training time when compared to MLP. Nonetheless, all four ML algorithms performed well and, in most cases, were able to achieve more than 90% accuracy. Moreover, confusion matrices were generated, confirming that the evaluated ML algorithms were able to classify most samples correctly. Other important metrics, such as precision, recall and F1-Score provided valuable insights into the ML algorithm performance for every output class.

As of now, the biggest limitation of SecRiskAI is the lack of real-world datasets to train the ML algorithms used in this work. To partially overcome this limitation and prove the effectiveness of the prototype, a synthetic dataset generation approach was followed, as described in the Data Gathering process. However, while synthetic data is able to mimic various properties and aspects of real data, it is usually very challenging to generate high-quality data for complex problems. If the generated dataset does not match the behaviour and properties of the real-world dataset, it will negatively impact the performance of the trained ML models.

Lastly, SecRiskAI is limited to assess the risk of only two types of cyber-attacks, namely DDoS and Phishing. To address this limitation, the current prototype was designed to be easily extensible, meaning that new ML models trained specifically for different types of cyber-attacks can be easily integrated into the current solution and exposed through the same API.

---

<sup>135</sup> <https://gitlab.ifl.uzh.ch/franco/ml-risk-smes>

## 6. Summary and Final Remarks

This Deliverable D4.3 presented the final overview of the cybersecurity threat landscape discussed by technological, legal/policy, and economic perspectives. The analysis surfaced existing gaps and challenges, described existing practices and countermeasures concerning the "state of play" of cybersecurity within organizations and put forward early recommendations of specific and broader relevance aiming to bridge those gaps identified between the "state of play" and the "state of the art" of cybersecurity.

Key findings of these Deliverables D4.1, D4.2, and D4.3 already contributed to the CONCORDIA roadmap, due at M48 by Task T4.4. Additionally, these findings provide relevant inputs from different perspectives to other CONCORDIA tasks, such as the "Code of Engagement of Threat Sharing Information" (WP3) and the cybersecurity consultant course creation and certification scheme (T3.4). A summary of key contributions and directions of relevance for next years in the light of respective technical, legal, and economic perspectives are shortly overviewed in the following.

### 6.1. Technical Views

Deliverable D4.3 provided the final discussion on the technical perspective of the CONCORDIA threat landscape. CONCORDIA threat landscape first analyzed current and emerging threats and evolving attacks in D4.1, updating them in D4.2 and D4.3. It then analyzed gaps and challenges with respect to identified threats in D4.2, updating them in D4.3. It finally analyzed countermeasures and research actions in this deliverable.

Some important key points emerged from the analysis done in this series of deliverables, which are reported in the following. The complexity of modern systems consisting of ever-increasing number of non-deterministic sensors and resource-constrained devices based on ML and AI models has no fixed topologies and set boundaries. Such systems integrate many technologies such as cloud, edge, IoT, 5G, SDN, thus pushing cybersecurity challenges to the extreme. Specialized security solutions must be enriched by horizontal approaches that evaluate the status and protect a system as a whole, ensuring minimum impact on the system itself that is often composed of minuscule sensors. Assurance and monitoring of modern systems are then key for system protection.

In this context, data assume a central role. Data are at the core of security solutions supporting the definition of high-quality detection and prevention techniques in all domains of interest. At the same time, data are the target of many attacks, which aim to reduce the quality of the decision support systems; for instance, data poisoning attacks and adversarial attacks that can target systems based on ML and AI to reduce the accuracy and precision of model inference. Data are therefore an invaluable weapon for cybersecurity experts, which need to master data science skills and competence in order to properly manage and analyse them. On the other side, data are fundamental to plan and implement disruptive attacks and need to be protected against poisoning and manipulation, when the target is an IT system, and against disinformation and misinformation when the target is an individual.

This scenario has then been further exacerbated by the COVID-19 pandemic that brought a significant increase in and worked as a multiplier of cyberattacks, which directly or indirectly involve threats to data. COVID-19 has in fact changed our normality accelerating the distribution of computations to homes and the 'periphery'. COVID-19 worked as a multiplier of the effects of existing threats such as social engineering, Distributed Denial of

Service (DDoS), ransomware, child sexual abuse material, to name but a few. More in deep, lockdown and smart working moved and distributed computation away from businesses' data centres, increasing the risk of loss and interception of information, data breaches, unauthorized acquisition of information, and malicious attacks in general. This new norm introduced the need for new security solutions based on the concept of "no trust, always verify".

On top of the above challenges, training and security awareness among organizations and end-users are two pillars of secure systems. They are of crucial importance for ensuring the further growth of IoT frameworks and virtualization platforms. Skill shortage is becoming more critical, since today single and not-expert users are directly involved in complex business processes and can influence them. Configuration errors are therefore increasing as never seen before, introducing a huge amount of new opportunities for cybercriminals to affect the CIA (Confidentiality, Integrity, Availability) properties of systems and users. Continuous training campaigns for employers are necessary to limit human errors due to non-adequate skills.

To conclude, many challenges exist and they can be classified in three areas: (i) technological challenges, including protection against persistent threats, insider threats, and AI-weaponized threats, untrusted environments, security of AI and ML models, network protection, cloud and virtualization security; (ii) human challenges, including protection against users' profiling, disinformation and misinformation, conscious use of social networks, training and awareness; (iii) organizational challenges, including distribution of responsibilities, lacks competences, tailored security investments.

## 6.2. Legal Views

The Legal Perspective encapsulated the policy and legal developments that took place at EU level since the submission of D4.2, in December 2021. Over the last year, cybersecurity has been found at the heart of the public discourse and a series of legislative initiatives have been undertaken by the European Regulator. Arguably, the proposed regulations complement the already applicable regulations and fall under strategic areas of the European Commission's policy agenda that pertain to Data Strategy and Cybersecurity Strategy. In this context, DGA and GDPR form clear examples of such complementarity, especially, in light of the Data Strategy, while -in light of the Cybersecurity Strategy- NIS2 and DORA are, also, complementing the latter being *lex specialis*. Certainly, cybersecurity is further regulated under other legislative instruments, such as the Chips Act and AI Act.

Nevertheless, the effectiveness of cybersecurity does not only depend on the statutory obligations, but -also- on how cybersecurity is implemented in reality through concrete practices. In this respect and as further evidenced by the series of interviews conducted in 2021, COVID-19 pandemic provided valuable insights as to how cybersecurity can be improved and on the necessity to establish digital sovereignty across the entire supply chain, especially, after the impact of COVID-19. To this end and acknowledging the reluctance within the cybersecurity domain to share information, especially, regarding threat intelligence, the Code of Engagement for Threat Intelligence Sharing was created initially to provide for CONCORDIA platform components. It is envisioned that other CONCORDIA partners and cybersecurity stakeholders, more broadly, adhere to the Code and that the Code creates, therefore, an impact within the community of cybersecurity even beyond the duration of CONCORDIA.

In terms of future work, T4.2 will keep monitoring the continuously changing EU policy and regulatory landscape and contribute accordingly to the final version of the Cybersecurity Roadmap, due under T4.4 at the end of the project.

### 6.3. Economic Views

The work developed within Task T4.3 in project year 3 introduced new approaches for the cybersecurity market's risk assessment, cyber insurance, and reputation systems. These approaches are supported by an overview of these fields, highlighting main challenges and opportunities. Also, Task T4.3 provided a framework composed out of the most relevant steps to guide companies in tasks related to cybersecurity planning and investments. This framework enables the summarization of the knowledge obtained in project years 1 to 3 and provides an umbrella for all these detailed approaches developed within cybersecurity planning and investment. Also, details of the economic issues related to the threat of information sharing were covered and discussed within T4.3.

The new solutions proposed within Deliverable D4.3 at hand focus on the analysis and support of the decision process for cybersecurity planning and investment from an economic perspective, thus, providing features and information to determine, plan, and deploy a cost-effective cybersecurity strategy in businesses, especially addressing SMEs. These solutions are supported by proof-of-concept implementations (*e.g.*, visualization tools for the risk assessment and investment recommendations, conversational agents as an interface for cybersecurity management in practice, cyber insurance models for companies, and blockchain-based approaches for the cybersecurity market), and pave the path for governments, industries, and other stakeholders to discuss and move toward a simplified and efficient way to adopt cybersecurity strategies.

Regarding the sustainability of Task T4.3 after the end of CONCORDIA (*i.e.*, after the project Year 4), it is relevant to consider two main lines: (a) the developed and extended solutions are already publicly available; thus, the community can base on these refined versions and can plan for deployments in real-world scenarios and (b) additional joint research and development proposals of the selected solutions can move on to the state of becoming new project proposals or the concept for new start-up businesses.

Besides that, challenges determined by Task 4.3 will approximately be present for the next 2-5 years. Those major and still not yet tackled challenges of cybersecurity planning and investments which are to be investigated and discussed by the European research community, focuses in the field of support. This support has to be addressed toward companies that operate with their business in the digital world and require an adequate cybersecurity strategy to protect their services, customers, and partners. Tools like those proposed within Task T4.3 (*e.g.*, SecRiskAI, MENTOR, and SERViz) can be integrated to cover the demands of cybersecurity planning with a cohesive data handling and easy-to-use-interfaces. Also, cyber insurance models (and reinsurance) will have a crucial role in maintaining businesses operating and helping them recover, even when cyberattacks are producing significant economic damage.

## References

- [1] L. Liu, O. De Vel, Q. Han, Z. J. and Y. Xiang, "Detecting and Preventing Cyber Insider Threats: A Survey," *IEEE Communication Surveys & Tutorials*, vol. 2, pp. 1390-1417, 2018.
- [2] M. F. Franco, B. Rodrigues, G. Parangi and B. Stiller, "Cybersecurity Threats, Stakeholders, and SEconomy Framework - An Economic Analysis for Cybersecurity," CONCORDIA T4.3 Report, Zürich, Switzerland, June, 2019.
- [3] S. Morgan, "Cybercrime To Cost The World \$10.5 Trillion Annually By 2025," 2020. [Online]. Available: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>.
- [4] L. Gordon, M. Loeb and L. Zhou, "Investing in Cybersecurity: Insights from the Gordon-Loeb Model," *Journal of Information Security*, vol. 1, no. 1, pp. 49-59, 2021.
- [5] M. Franco, B. Rodrigues, E. Scheid, C. Killer, A. Jacobs, L. Granville and B. Stiller, "SecBot: a Business-Driven Conversational Agent for Cybersecurity Planning and Management," in *16th International Conference on Network and Service Management (CNSM 2020)*, Izmir, Turkey, 2020.
- [6] Cynet, "Survey of CISOs with Small Cyber Security Teams," 2021. [Online]. Available: <https://hubs.ly/H0FrnJ40>.
- [7] European Union Agency for Cybersecurity (ENISA), "Cybersecurity for SMEs: Challenges and Recommendations," 2021. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>.
- [8] M. Anisetti, C. Ardagna, M. Cremonini, E. Damiani, J. Sessa and L. Costa, "Security Threat Landscape," 2020. [Online]. Available: [https://www.concordia-h2020.eu/wp-content/uploads/2021/03/White\\_paper\\_SecurityThreats.pdf](https://www.concordia-h2020.eu/wp-content/uploads/2021/03/White_paper_SecurityThreats.pdf).
- [9] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2021," 2021. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>.
- [10] P. Pagani, *Cyber Defense Magazine (CDM)*, Cyber Defense Media Group, 2019.
- [11] H. Ö. a. B. Otto, "Consortium Research: A Method for Researcher Practitioner Collaboration in Design-Oriented IS Research," *Business & Information Systems Engineering*, vol. 2, no. 5, pp. 286-293, 2010.
- [12] F. X. Vinel, L. Yang and L. A. Wang, "Internet of Things," *International Journal of Communication Systems*, vol. 9, pp. 1101-1102, 2012.
- [13] M. Litoussi, N. Kannouf, K. El Makkaoui, A. Ezzati and M. Fartitchou, "IoT security: challenges and countermeasures," *Procedia Computer Science*, vol. 177, pp. 503-508, 2020.
- [14] L. Tawalbeh, F. Muheidat, M. Tawalbeh and M. a. o. Quwaider, "IoT Privacy and security: Challenges and solutions," *Applied Sciences*, vol. 10, no. 12, p. 4102, 2020.
- [15] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 336-341, 2015.

- [16] M. Patton, E. Gross, R. Chinn, S. Forbis, L. Walker and H. Chen, "Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT)," *Joint Intelligence and Security Informatics Conference (JISIC)*, pp. 232-235, 2014.
- [17] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for IoT," *Applied Soft Computing*, vol. 72, pp. 79-89, 2018.
- [18] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Generation Computer Systems*, vol. 82, pp. 761-768, 2018.
- [19] A. Abeshu and N. Chilamkurti, "Deep learning: The frontier for distributed attack detection in fog-to-things computing," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 169-175, 2018.
- [20] J. Ye, X. Cheng, J. Zhu, L. Feng and L. Song, "A DDoS attack detection method based on SVM in software defined network," *Security and Communication Networks*, vol. 2018, 2018.
- [21] S. Tomovic, K. Yoshigoe, I. Maljevic and I. Radusinovic, "Software-defined fog network architecture for IoT," *Wireless Personal Communications*, vol. 92, no. 1, pp. 181-196, 2017.
- [22] R. Kokila, S. T. Selvi and K. Govindarajan, "DDoS detection and analysis in SDN-based environment using support vector machine classifier," *2014 Sixth International Conference on Advanced Computing (ICoAC)*, pp. 205-210, 2014.
- [23] J. Canedo and A. Skjellum, "Using machine learning to secure IoT systems," *2016 14th annual conference on privacy, security and trust (PST)*, pp. 219-222, 2016.
- [24] N. Nesa, T. Ghosh and I. Banerjee, "Non-parametric sequence-based learning approach for outlier detection in IoT," *Future Generation Computer Systems*, vol. 82, pp. 412-421, 2018.
- [25] J. Kim, J. Kim, H. L. T. Thu and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," in *2016 International Conference on Platform Technology and Service (PlatCon)*, IEEE, 2016, pp. 1-5.
- [26] A. Saeed, A. Ahmadinia, A. Javed and H. Larijani, "Intelligent intrusion detection in low-power IoTs," *ACM Transactions on Internet Technology (TOIT)*, vol. 16, no. 4, pp. 1-25, 2016.
- [27] P. M. Shakeel, S. Baskar, V. S. Dhulipala, S. Mishra and M. M. Jaber, "Maintaining security and privacy in health care system using learning based deep-Q-networks," *Journal of medical systems*, vol. 42, no. 10, pp. 1-10, 2018.
- [28] F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," *IEEE Communications Surveys Tutorials*, vol. 22, no. 3, pp. 1686-1721, 2020.
- [29] J. Domanska, E. Gelenbe, T. Czachorski, A. Drosou and D. Tzovaras, "Research and innovation action for the security of the internet of things: The seriot project," *International ISCIS Security Workshop*, pp. 101-118, 2018.
- [30] C. Lin, D. He, X. Huang, K.-K. R. Choo and A. V. Vasilakos, "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *Journal of Network and Computer Applications*, vol. 116, pp. 42-52, 2018.
- [31] S. N. Mohanty, K. Ramya, S. S. Rani, D. Gupta, K. Shankar, S. Lakshmanaprabu and A. Khanna, "An efficient Lightweight integrated Blockchain (ELIB) model for

- IoT security and privacy,” *Future Generation Computer Systems*, vol. 102, pp. 1027-1037, 2020.
- [32] S. K. Singh, S. Rathore and J. H. Park, “Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence,” *Future Generation Computer Systems*, vol. 110, pp. 721-743, 2020.
- [33] M. El-Hajj, A. Fadlallah, M. Chamoun and A. Serhrouchni, “A survey of internet of things (IoT) authentication schemes,” *Sensors*, vol. 19, no. 5, p. 1141, 2019.
- [34] T. W. Chim, S.-M. Yiu, L. C. Hui and V. O. Li, “PASS: Privacy-preserving authentication scheme for smart grid network,” *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 196-201, 2011.
- [35] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu and X. Shen, “Towards a light-weight message authentication mechanism tailored for smart grid communications,” *2011 IEEE conference on computer communications workshops (INFOCOM WKSHPs)*, pp. 1018-1023, 2011.
- [36] H. Nicanfar, P. Jokar, K. Beznosov and V. C. Leung, “Efficient authentication and key management mechanisms for smart grid communications,” *IEEE systems journal*, vol. 8, no. 2, pp. 629-640, 2013.
- [37] C. Ji, J. Kim, J.-Y. Lee and M. Hong, “Review of one-time signatures for multicast authentication in smart grid,” in *2015 12th International Conference & Expo on Emerging Technologies for a Smarter World (CEWIT)*, IEEE, 2015, pp. 1-4.
- [38] H. Xu, J. Ding, P. Li, F. Zhu and R. Wang, “A lightweight RFID mutual authentication protocol based on physical unclonable function,” *Sensors*, vol. 18, no. 3, p. 760, 2018.
- [39] P. Tuyls and L. Batina, “RFID-tags for anti-counterfeiting,” in *Cryptographers’ track at the RSA conference*, Springer, 2006, pp. 115-131.
- [40] P. Gope, J. Lee and T. Q. Quek, “Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2831-2843, 2018.
- [41] C. Huth, J. Zibuschka, P. Duplys and T. Guneyusu, “Securing systems on the Internet of Things via physical properties of devices and communications,” in *2015 Annual IEEE Systems Conference (SysCon) Proceedings*, IEEE, 2015, pp. 8-13.
- [42] M. Zhao, X. Yao, H. Liu and H. Ning, “Physical unclonable function based authentication protocol for unit IoT and ubiquitous IoT,” in *2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)*, IEEE, 2016, pp. 179-184.
- [43] M. A. Muhal, X. Luo, Z. Mahmood and A. Ullah, “Physical unclonable function based authentication scheme for smart devices in Internet of Things,” in *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)*, IEEE, 2018, pp. 160-165.
- [44] D. Mukhopadhyay, “PUFs as promising tools for security in Internet of Things,” *IEEE Design & Test*, vol. 33, no. 3, pp. 103-115, 2016.
- [45] J. R. Wallrabenstein, “Practical and secure IoT device authentication using physical unclonable functions,” in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, IEEE, 2016, pp. 99-106.
- [46] M. Barbareschi, P. Bagnasco and A. Mazzeo, “Authenticating IoT devices with physically unclonable functions models,” in *2015 10th International Conference on*

- P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, IEEE, 2015, pp. 563-567.
- [47] C. Schmitt, M. Noack and B. Stiller, "TinyTO: Two-way authentication for constrained devices in the Internet of Things," in *Internet of Things*, Elsevier, 2016, pp. 239-258.
- [48] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," in *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, IEEE, 2014, pp. 2728-2733.
- [49] M. Turkanovi}, B. Brumen and M. Holbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Networks*, vol. 20, pp. 96-112, 2014.
- [50] M. Alotaibi, "An enhanced symmetric cryptosystem and biometric-based anonymous user authentication and session key establishment scheme for WSN," *IEEE Access*, vol. 6, pp. 70072-70087, 2018.
- [51] D. R. McKinnel, T. Dargahi, A. Dehghantanha and K.-K. R. Choo, "A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment," *Computers & Electrical Engineering*, vol. 75, pp. 175-188, 2019.
- [52] J. Schwartz and H. Kurniawati, "Autonomous penetration testing using reinforcement learning," *arXiv preprint arXiv:1905.05965*, 2019.
- [53] M. C. Ghanem and T. M. Chen, "Reinforcement learning for efficient network penetration testing," *Information*, vol. 11, no. 1, p. 6, 2020.
- [54] J. Jacobs, S. Romanosky, B. Edwards, M. Roytman and I. Adjerid, "Exploit prediction scoring system (EPSS)," *arXiv preprint arXiv:1908.04856*, 2019.
- [55] J. Jacobs, S. Romanosky, I. Adjerid and W. Baker, "Improving vulnerability remediation through better exploit prediction," *Journal of Cybersecurity*, vol. 6, no. 1, p. tyaa015, 2020.
- [56] Y. Fang, Y. Liu, C. Huang and L. Liu, "FastEmbed: Predicting vulnerability exploitation possibility based on ensemble machine learning algorithm," *Plos one*, vol. 15, no. 2, p. e0228439, 2020.
- [57] G. Karatas, O. Demir and O. K. Sahingoz, "Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset," *IEEE Access*, vol. 8, pp. 32150--32162, 2020.
- [58] E. Nunes, A. Diab, A. Gunn, E. Marin, V. Mishra, V. Paliath, J. Robertson, J. Shakarian, A. Thart and P. Shakarian, "Darknet and deepnet mining for proactive cybersecurity threat intelligence," in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, IEEE, 2016, pp. 7-12.
- [59] U. Noor, Z. Anwar, T. Amjad and K.-K. R. Choo, "A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise," *Future Generation Computer Systems*, vol. 96, pp. 227-242, 2019.
- [60] T. Shapira and Y. Shavitt, "A Deep Learning Approach for IP Hijack Detection Based on ASN Embedding," in *Proceedings of the Workshop on Network Meets AI & ML*, 2020, pp. 35-41.
- [61] D. Ott and C. a. o. Peikert, "Identifying research challenges in post quantum cryptography migration and cryptographic agility," *arXiv preprint arXiv:1909.07353*, 2019.

- [62] S. Brohi, M. Bamiah, M. Brohi and R. Kamran, "Identifying and Analyzing Security Threats to Virtualized Cloud Computing Infrastructures.," *Proceedings of International of Cloud Computing, Technologies, Applications & Management*, pp. 151-155, 2012.
- [63] A. F. S. Althobaiti, "Analyzing security threats to virtual machines monitor in cloud computing environment," *Journal of Information Security*, vol. 8, no. 01, p. 1, 2017.
- [64] A. Iqbal, C. Pattinson and A.-L. Kor, "Performance Monitoring of Virtual Machines (VMs) of Type I and II hypervisors with SNMPv3.," *World Congress on Sustainable Technologies (WCST)*, pp. 98-99, 2015.
- [65] D. Ferraiolo, J. Cugini and D. R. Kuhn, "Role-based access control (RBAC): Features and motivations," in *Proceedings of 11th annual computer security application conference*, 1995, pp. 241-48.
- [66] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE symposium on security and privacy (SP'07)*, IEEE, 2007, pp. 321-334.
- [67] C. B. Tan, M. H. A. Hijazi, Y. Lim and A. Gani, "A survey on Proof of Retrievability for cloud data integrity and availability: Cloud storage state-of-the-art, issues, solutions and future trends," *Journal of Network and Computer Applications*, vol. 110, pp. 75-86, 2018.
- [68] D. Quick, B. Martini and R. Choo, *Cloud storage forensics*, Syngress, 2013.
- [69] S. Khan, S. Parkinson and Y. Qin, "Fog computing security: a review of current applications and security solutions," *Journal of Cloud Computing*, vol. 6, no. 1, pp. 1-22, 2017.
- [70] D. B. Rawat, R. Doku and M. Garuba, "Cybersecurity in big data era: From securing big data to data-driven security," *IEEE Transactions on Services Computing*, 2019.
- [71] L. Yue, H. Junqin, Q. Shengzhi and W. Ruijin, "Big data model of security sharing based on blockchain," *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)*, pp. 117-121, 2017.
- [72] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757-14767, 2017.
- [73] U. U. Uchibeke, K. A. Schneider, S. H. Kassani and R. Deters, "Blockchain Access Control Ecosystem for Big Data Security," *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1373-1378, 2018.
- [74] J. Kepner, V. Gadepally, P. Michaleas, N. Schear, M. Varia, A. Yerukhimovich and R. K. Cunningham, "Computing on Masked Data: a High Performance Method for Improving Big Data Veracity," *2014 IEEE High Performance Extreme Computing Conference (HPEC)*, pp. 1-6, 2014.
- [75] D. Wang, B. Guo, Y. Shen, S.-J. Cheng and Y.-H. Lin, "A Faster Fully Homomorphic Encryption Scheme in Big Data," *2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA)*, pp. 345-349, 2017.
- [76] T. B. Patil, G. K. Patnaik and A. T. Bhole, "Big data privacy using fully homomorphic non-deterministic encryption," in *2017 IEEE 7th International Advance Computing Conference (IACC)*, IEEE, 2017, pp. 138-143.

- [77] T. Yang, P. Shen, X. Tian and C. Chen, "A Fine-Grained Access Control Scheme for Big Data Based on Classification Attributes," in *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, IEEE, 2017, pp. 238-245.
- [78] A. Kulkarni, C. Shea, H. Homayoun and T. Mohsenin, "Less: Big Data Sketching and Encryption on Low Power Platform," *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*, pp. 1631-1634, 2017.
- [79] A. Gupta, A. Verma, P. Kalra and L. Kumar, "Big Data: A security compliance model," in *2014 Conference on IT in Business, Industry and Government (CSIBIG)*, IEEE, 2014, pp. 1-5.
- [80] A. Al-Shomrani, F. Fathy and K. Jambi, "Policy enforcement for big data security," *2017 2nd international conference on anti-cyber crimes (icacc)*, pp. 70-74, 2017.
- [81] N.-Y. Lee and B.-H. Wu, "Privacy protection technology and access control mechanism for medical big dat," *2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*, pp. 424-429, 2017.
- [82] N. Papernot, P. McDaniel, A. Sinha and M. Wellman, "Towards the science of security and privacy in machine learning," *arXiv preprint arXiv:1611.03814*, 2016.
- [83] W. Xu, D. Evans and Y. Qi, "Feature squeezing: Detecting adversarial examples in deep neural networks," *arXiv preprint arXiv:1704.01155*, 2017.
- [84] S. Pissanetzky, "On the future of information: Reunification, computability, adaptation, cybersecurity, semantics," *IEEE Access*, vol. 4, pp. 1117-1140, 2016.
- [85] R. Geambasu, T. Kohno, A. A. Levy and H. M. Levy, "Vanish: Increasing Data Privacy with Self-Destructing Data.," in *USENIX security symposium*, vol. 316, 2009.
- [86] M. Franco, "CyberTEA: a Technical and Economic Approach for the Cybersecurity Planning and Investment," PhD Thesis, University of Zurich, Zurich, Switzerland, 2022 (Work in Progress).
- [87] Project Management Institute, *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*, 7th edition ed., Pennsylvania: Project Management Institute, 2017.
- [88] M. Franco, B. Rodrigues and S. Burkhard, "MENTOR: The Design and Evaluation of a Protection Services Recommender System," in *15th International Conference on Network and Service Management (CNSM 2019)*, Halifax, Canada, 2019.
- [89] W. Sonnenreich, J. Albanese and B. Stout, "Return On Security Investment (ROSI): a Practical Quantitative Model," *Journal of Research and Practice in Information Technology*, vol. 1, no. 1, pp. 239-252, 2005.
- [90] K. Nir, "The Economics of Cyber-Insurance," *IT Professional*, vol. 20, no. 6, pp. 9-14, 2018.
- [91] R. Pal, L. Golubchik, K. Psounis and P. Hui, "Will Cyber-Insurance Improve Network Security? A Market Analysis," in *IEEE Conference on Computer Communications (INFOCOM 2014)*, Toronto, Canada, 2014.
- [92] Munich Re, "Cyber Insurance: Risks and Trends 2021," June 2021. [Online]. Available: <https://www.munichre.com/topics-online/en/digitalisation/cyber/cyber-insurance-risks-and-trends-2021.html>.
- [93] AmTrust, "Cyber Insurance Market Growth," June 2021. [Online]. Available: <https://amtrustfinancial.com/blog/agents/growth-of-the-cyber-insurance-market-agents>.

- [94] J. R. Nurse, L. Axon, A. Erola, I. Agrafiotis, M. Goldsmith and S. Creese, "The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes," in *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA 2020)*, Dublin, Ireland, 2020.
- [95] M. Franco, N. Berni, E. Scheid, C. Killer, B. Rodrigues and B. Stiller, "SaCI: a Blockchain-based Cyber Insurance Approach for the Deployment and Management of a Contract Coverage," in *18th International Conference on the Economics of Grids, Clouds, Systems and Services (GECON 2021)*, Virtually, 2021.
- [96] E. Anggraeni, E. Hartigh and M. Zegveld, "Business Ecosystem as a Perspective for Studying the Relations between Firms and their Business Networks," in *ECCON 2007*, Veldhoven, Netherlands, 2007.
- [97] S. Wieninger, R. Götzen, G. Gudergan and K. Wenning, "The Strategic Analysis of Business Ecosystems: New Conception and Practical Application of a Research Approach," in *IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, Valbonne Sophia-Antipolis, France, 2019.
- [98] S. Vicini, F. Alberti, N. Notario, J. R. Pastoriza and A. Sanna, "Co-creating Security-and-Privacy-by-Design Systems," in *11th International Conference on Availability, Reliability and Security (ARES)*, Salzburg, Austria, 2016.
- [99] T. Noe and G. Parker, "Winner Take All: Competition, Strategy, and the Structure of Returns in the Internet Economy," *Journal of Economics & Management Strategy*, vol. 14, no. 1, pp. 141-164, 2005.
- [100] J. Arkkio, "The Influence of Internet Architecture on Centralised Versus Distributed Internet Services," *Journal of Cyber Policy*, vol. 1, no. 5, pp. 30-45, 2020.
- [101] SAINT, "SAINT Project," [Online]. Available: <https://project-saint.eu/>.
- [102] NIST, "Guide to Cyber Threat Information Sharing (Special Publication 800-150)," 2016.
- [103] I. Vakilinia, S. Louis and S. Sengupta, "Evolving Sharing Strategies in Cybersecurity Information Exchange Framework," in *Genetic and Evolutionary Computation Conference Companion (GECCO)*, 2017.
- [104] W. Zhao and G. White, "Designing a Formal Model Facilitating Collaborative Information Sharing for Community Cyber Security," in *47th Hawaii International Conference on System Sciences*, Hawaii, 2014.
- [105] W. Zhao and G. White, "An Evolution Roadmap for Community Cyber Security Information Sharing Maturity Model," in *50th HICSS 2017*., Waikoloa Village, Hawaii, USA, 2017.
- [106] Z. Rashid, U. Noor and J. Altmann, "Economic Model for Evaluating the Value Creation Through Information Sharing within the Cybersecurity Information Sharing Ecosystem," *Future Generation Computer Systems*, vol. 124, pp. 436-466, 2021.
- [107] Z. Rashid, U. Noor and J. Altmann, "Network Externalities in Cybersecurity Information Sharing Ecosystems," in *GECON 2018*, Pisa, Italy, 2018.
- [108] O. Al-Ibrahim, A. Mohaisen, C. Kamhoua, K. Kwiat and L. Njilla, *Beyond Free Riding: Quality of Indicators for Assessing Participation in Information Sharing for Threat Intelligence*, arXiv, 2017.
- [109] M. He, L. Devine and J. and Zhuang, "Perspectives on Cybersecurity Information Sharing among Multiple Stakeholders Using a Decision-Theoretic Approach," *Risk Analysis*, vol. 38, pp. 215-225, 2018.

- [110] P. Koepke, *Cybersecurity Information Sharing Incentives and Barriers (Working Paper)*, 2017.
- [111] A. Mermoud, M. Keupp, S. Huguenin, M. K. Palmié and D. P. David, “Incentives for Human Agents to Share Security Information: a Model and an Empirical Test,” in *7th Workshop on the Economics of Information Security (WEIS)*, Innsbruck, Austria, 2018.
- [112] Ponemon, “The Value of Threat Intelligence: Annual Study of North American & United Kingdom Companies,” 2019.
- [113] R. Garrido-Pelaz, L. González-Manzano and s. Pastrana, “Shall We Collaborate? A Model to Analyse the Benefits of Information Sharing,” in *ACM on Workshop on Information Sharing and Collaborative Security (WISCS '16)*, New York, USA, 2016.
- [114] HERMENEUT, “Project Web Site,” [Online]. Available: <https://www.hermeneut.eu/>.
- [115] NSCS, “Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts,” NSCS Report, 2019.
- [116] SISSDEN , “Company Web Site,” [Online]. Available: <https://sisssden.com/>.
- [117] Mckinsey, “The Risk-based Approach to Cybersecurity,” 2019. [Online]. Available: <https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity>.
- [118] Gartner, “Implement a Risk-Based Approach to Vulnerability Management,” 2018.
- [119] APWG, “Phishing Activity Trends Report: Activity October-December 2020,” 2021.
- [120] E. Scheid, B. Rodrigues, C. Killer, M. Franco, S. Rafati and B. Stiller, “Blockchains and Distributed Ledgers Uncovered: Clarifications, Achievements, and Open Issues,” in *Advancing Research in Information and Communication Technology*, Cham, Springer, 2021, pp. 1-29.
- [121] A. Charle and M. Franco, *Decentralized Reputation and SLA Enforcement for Cybersecurity*, Zurich, Switzerland: Communication Systems Group, 2020.
- [122] S. M. Pappalardo, M. Niemiec, M. Bozhilova, N. Stoianov, A. Dziech and B. Stiller, “Multi-Sector Assessment Framework - A New Approach to Analyse Cybersecurity Challenges and Opportunities,” in *International Conference on Multimedia Communications, Services and Security*, Kraków, Poland, 2020.
- [123] Deloitte, “Why Artificial Intelligence is a Game Changer for Risk Management.,” Deloitte, London, United Kingdom, 2021.
- [124] M. F. Franco, E. Sula, A. Huertas, E. J. Scheid, L. Z. Granville and B. Stiller, “SecRiskAI: a Machine Learning-Based Approach for Cybersecurity Risk Prediction in Businesses,” in *24th IEEE International Conference on Business Informatics*, Amsterdam, The Netherlands, 2022.
- [125] M. Hittmeir, A. Ekelhart and R. Mayer, “On the Utility of Synthetic Data: An Empirical Evaluation on Machine Learning Tasks,” in *14th International Conference on Availability, Reliability and Security (ARES 2019)*, Canterbury, United Kingdom, 2019.
- [126] Department of Homeland Security’s (DHS), “Homeland Security: Cybersecurity Advisors,” 2017. [Online]. Available: [https://www.bu.edu/tech/files/2017/09/DHS\\_CSA\\_Fact\\_Sheet\\_2017-1.pdf](https://www.bu.edu/tech/files/2017/09/DHS_CSA_Fact_Sheet_2017-1.pdf).

- [127] J. Heaton, “The Number of Hidden Layers,” 2017. [Online]. Available: <https://www.heatonresearch.com/2017/06/01/hidden-layers.html>.
- [128] M. Franco, E. Sula, B. Rodrigues, E. Scheid and B. Stiller, “ProtectDDoS: A Platform for Trustworthy Offering and Recommendation of Protections,” in *International Conference on Economics of Grids, Clouds, Software and Services (GECON 2020)*, Izola, Slovenia, 2020.
- [129] E. Sula, M. Franco and B. Stiller, “SecRiskAI: A Machine Learning-based Tool for Cybersecurity Risk Assessment,” Universität Zürich, Communication Systems Group, Department of Informatics, Zürich, Switzerland, 2021.

All of the links provided above were last accessed on November 10, 2021.

## Appendices

### A. Threats, Gaps, Challenges, Countermeasures, Research Actions: Summary

The following sections present a summary of the threats, gaps, challenges, countermeasures, and research actions emerging from the analysis in D4.1, D4.2, and D4.3.

#### A.1. Device/IoT-Centric Security

Table 8 presents the complete mapping between assets, threats, and gaps in Device/IoT domain using the threat notation of D4.1 (T<domain number>.<threat group number>.<threat number>) and the gap and challenge notation of D4.2 (T<domain number>.<gap number>).

Table 8: Mapping Assets, Threats and Gaps in the Device/IoT Domain

Threat Group (TG)	Threat (T)	Asset (A)	Gaps (G)
Unintentional damage/loss of information or IT assets (1)	Information leakage/sharing due to human errors (1)	Data, Device, Infrastructure, Platform and backend, Decision making	G1.5 - Lack of awareness and knowledge (skill shortage) G1.7 - Lack of security-dedicated budget
	Inadequate design and planning or incorrect adaptation (2)	Device, Infrastructure, Platform and backend, Management	G1.1 - Gaps in design, G1.7 - Lack of security-dedicated budget
	Inadequate design and planning or incorrect adaptation in the critical scenario – COVID-19 (3)		G1.1 - Gaps in design G1.10 - Gaps in cyber hygiene practices G1.11 - Gaps in handling critical scenarios
Interception and unauthorized acquisition (2)	Interception of information (1)	Device, Infrastructure, Security mechanisms	G1.3 - Gaps on authorization and authentication G1.6: Lack of interoperability G1.12 – Gaps in insufficient data protection (communication and storage)
	Unauthorized acquisition of information (2)	Device, Infrastructure, Platform, and backend	G1.3 - Gaps on authorization and authentication G1.11 - Gaps in handling critical scenarios

			G1.12 - Gaps in insufficient data protection (communication and storage)
Intentional Physical Damage (3)	Device modification (1)	Device, Infrastructure	G1.7 - Lack of security-dedicated budget G1.4 - Gaps on diagnosis and response capabilities
	Extraction of private information (2)	Device	G1.2 - Gaps on protection mechanisms adoption and hardening
	Lack of control on safety implications – COVID-19 (3)		G1.7: Lack of security-dedicated budget G1.2 - Gaps on protection mechanisms adoption and hardening
Nefarious activity/abuse (4)	Identity fraud (1)	Device, Infrastructure, Platform, and backend	G1.3 - Gaps on authorization and authentication G1.12 – Gaps in insufficient data protection (communication and storage)
	Denial of service (2)	Device, Infrastructure, Security mechanisms, Platform, and backend	G1.1 - Gaps in design G1.11 - Gaps in handling critical scenarios
	Malicious code/software /activity (3)	Device, Infrastructure, Security mechanisms, Platform and backend	G1.2 - Gaps on protection mechanisms adoption and hardening G1.9 - Product lifecycle management leakages
	Misuse of assurance tools (4)	Data, Devices, Platform and backend, Infrastructure, Security Mechanisms, Management	G1.7 - Lack of security-dedicated budget G1.1 - Gaps in design G1.9 - Product lifecycle management leakages
	Failures of business process (5)	Devices, Platform and backend, Infrastructure, Security Mechanisms, Management	G1.4 - Gaps on diagnosis and response capabilities G1.6 - Lack of interoperability G1.8 - Fragmentation in security approaches and regulations G1.13 - Gaps in device management and the

			use of outdated components
	Code execution and injection (unsecured APIs) (6)	Platform and backend, Security Mechanisms, Management.	G1.2 - Gaps on protection mechanisms adoption and hardening G1.9 - Product lifecycle management leakages
	Device hijacking (7)	Device, Infrastructure	G1.1 - Gaps in design G1.2 - Gaps on protection mechanisms adoption and hardening G1.12 - Gaps in insufficient data protection (communication and storage)
	Social engineering (8)	Data, Device	G1.3 - Gaps on authorization and authentication G1.5 - Lack of awareness and knowledge (skill shortage) G1.12 - Gaps in insufficient data protection (communication and storage)
Legal (5)	Violation of laws or regulations (1)	all	G1.6 - Lack of interoperability G1.8 - Fragmentation in security approaches and regulations
Organizational threats (6)	Skill shortage (1)	Roles	G1.5 - Lack of awareness and knowledge (skill shortage) G1.7 - Lack of security-dedicated budget
	Lack of strong cyber hygiene practices – COVID-19 (2)		G1.7 - Lack of security-dedicated budget G1.10 - Gaps in cyber hygiene practices G1.13 - Gaps in device management and the use of outdated components

Table 9 provides a binding between identified threats, gaps/challenges, countermeasures, and research actions.

Table 9: Mapping Threats, Gaps, Countermeasures, Research Actions

<b>Threat (T)</b>	<b>Gap (G)</b>	<b>Countermeasure (C)</b>	<b>Research Action (RA)</b>
T1.1.1 - Information leakage/sharing due to human errors	G1.5 - Lack of awareness and knowledge (skill shortage) G1.7: Lack of security-dedicated budget	C1.2 - Implementing segmentation C1.10 - Raising security awareness	RA1.2 - Blockchain-based solutions RA1.3 - Novel authentication schemes
T1.1.2 - Inadequate design and planning or incorrect adaptation	G1.1 - Gaps in design G1.7 - Lack of security-dedicated budget	C1.8 – Testing C1.9 - Fostering security-by-design approach	RA1.3 - Novel authentication schemes
T1.1.3 - Inadequate design and planning or incorrect adaptation in the critical scenario - COVID-19	G1.1 - Gaps in design G1.10 - Gaps in cyber hygiene practices G1.11 - Gaps in handling critical scenarios	C1.8 – Testing C1.9 - Fostering security-by-design approach	RA1.1 - ML/DL-based solutions RA1.3 – Novel authentication schemes
T1.2.1 - Interception of information	G1.3 - Gaps on authorization and authentication G1.6 - Lack of interoperability G1.12 - Gaps in insufficient data protection (communication and storage)	C1.2 - Implementing segmentation C1.3 - Ensuring device authentication C1.4 - Deploying Public Key Infrastructure (PKI)	RA1.1 - ML/DL-based solutions RA1.3 – Novel authentication schemes
T1.2.2 - Unauthorized acquisition of information (data breach)	G1.3 - Gaps on authorization and authentication G1.11 - Gaps in handling critical scenarios G1.12 - Gaps in insufficient data protection (communication and storage)	C1.2 - Implementing segmentation C1.3 - Ensuring device authentication C1.4 - Deploying Public Key Infrastructure (PKI)	RA1.1 - ML/DL-based solutions RA1.3 - Novel authentication schemes
T1.3.1 - Device modification	G1.3 - Gaps on authorization and authentication G1.12 - Gaps in insufficient data protection (communication and storage)	C1.11 - Firmware maintenance and integrity	RA1.1 - ML/DL-based solutions RA1.2 - Blockchain-based solution
T1.3.2 - Extraction of private information	G1.2 - Gaps on protection mechanisms adoption and hardening	C1.2 - Implementing segmentation C1.3 - Ensuring device authentication	RA1.1 - ML/DL-based solutions

		C1.4 - Deploying Public Key Infrastructure (PKI)	
T1.3.3 - Lack of control on safety implications - COVID-19	G1.2 - Gaps on protection mechanisms adoption and hardening G1.7 - Lack of security-dedicated budget	C1.1 - Performing contextual vulnerability assessment C1.2 - Implementing segmentation, C1.6 - Utilizing security analytics, monitoring, and risk assessment techniques C1.10 - Raising security awareness C1.12 - Enforcing regulations	RA1.1 - ML/DL-based solutions RA1.2 - Blockchain-based solution
T1.4.1 - Identity fraud	G1.3 - Gaps on authorization and authentication G1.12 - Gaps in insufficient data protection (communication and storage)	C1.3 - Ensuring device authentication	RA1.3 - Novel authentication schemes
T1.4.2 - Denial of service	G1.1 - Gaps in design G1.11 - Gaps in handling critical scenarios	C1.1 - Performing contextual vulnerability assessment C1.5 - Deploying AI and machine learning C1.7 - Utilizing SDN with IoT, C1.8 - Testing	RA1.1 - ML/DL-based solutions RA1.2 - Blockchain-based solution RA1.3 - Novel authentication schemes
T1.4.3 - Malicious code/software/activity	G1.2 - Gaps on protection mechanisms adoption and hardening G1.9 - Product lifecycle management leakages	C1.1 - Performing contextual vulnerability assessment C1.5 - Deploying AI and machine learning C1.6 - Utilizing security analytics, monitoring, and risk assessment techniques C1.7 - Utilizing SDN with IoT	RA1.1 - ML/DL-based solutions RA1.2 - Blockchain-based solution

T1.4.4 - Misuse of assurance tools	G1.7 - Lack of security-dedicated budget G1.1 - Gaps in design G1.9 - Product lifecycle management leakages	C1.9 - Fostering security-by-design approach C1.12 - Enforcing regulations	RA1.1 - ML/DL-based solutions RA1.3 - Novel authentication schemes
T1.4.5 - Failures of business process	G1.4 - Gaps on diagnosis and response capabilities G1.6 - Lack of interoperability G1.8 - Fragmentation in security approaches and regulations G1.13 - Gaps in device management and the use of outdated components	C1.9 - Fostering security-by-design approach C1.10 - Raising security awareness	RA1.1 - ML/DL-based solutions RA1.2 - Blockchain-based solution
T1.4.6 - Code execution and injection (unsecured APIs)	G1.2 - Gaps on protection mechanisms adoption and hardening G1.9 - Product lifecycle management leakages	C1.1 - Performing contextual vulnerability assessment C1.5 - Deploying AI and machine learning C1.6 - Utilizing security analytics, monitoring, and risk assessment techniques C1.7 - Utilizing SDN with IoT C1.11 - Firmware maintenance and integrity	RA1.1 - ML/DL-based solutions
T1.4.7 - Device hijacking	G1.1 - Gaps in design G1.2 - Gaps on protection mechanisms adoption and hardening G1.12 - Gaps in insufficient data protection (communication and storage)	C1.2 - Implementing segmentation C1.3 - Ensuring device authentication C1.4 - Deploying Public Key Infrastructure (PKI) C1.7 - Utilizing SDN with IoT C1.11 - Firmware maintenance and integrity	RA1.3 - Novel authentication schemes
T1.4.8 – Social engineering	G1.3 - Gaps on authorization and authentication G1.5 - Lack of awareness and knowledge (skill shortage)	C1.10 - Raising security awareness	RA1.3 - Novel authentication schemes

	G1.12 - Gaps in insufficient data protection (communication and storage)		
T1.5.1 - Violation of laws or regulations	G1.6 - Lack of interoperability G1.8 - Fragmentation in security approaches and regulations	C1.10 - Raising security awareness	RA1.2 - Blockchain-based solution
T1.6.1 - Skill shortage	G1.5 - Lack of awareness and knowledge (skill shortage) G1.7 - Lack of security-dedicated budget	C1.12 - Enforcing regulations	RA1.2 - Blockchain-based solution
T1.6.2 - Lack of strong cyber hygiene practices – COVID-19	G1.7 - Lack of security-dedicated budget G1.10 - Gaps in cyber hygiene practices G1.13 – Gaps in device management and the use of outdated components	C1.10 - Raising security awareness	RA1.2 - Blockchain-based solution

### A.2. Network-Centric Security

Table 10 presents the complete mapping between assets, threats, and gaps in the Network domain using the threat notation of D4.1 (T<domain number>.<threat group number>.<threat number>) and the gap and challenge notation of D4.2 (T<domain number>.<gap number>).

Table 10: Mapping Assets, Threats and Gaps in Network Domain

Threat Group (TG)	Threat (T)	Asset (A)	Gaps (G)
Unintentional damage/loss of information or IT assets (1)	Erroneous use or administration of devices and systems (1)	Core Network, Access Network, Infrastructure Network, Peering Points	G2.2 – Gaps on continuous hardening & patching of IT systems G2.3 – Gaps on security training and awareness toward employees G2.16 – Gaps on Security of the new Open Radio Access Network model
	Security misconfigurations in systems/networks (2)	Core Network, Access Network, Infrastructure Network, Peering Points	G2.2 – Gaps on continuous hardening & patching of IT systems G2.5 – Gaps in the standardization process to include formal security verification and security assessment/testing of new protocol/network specifications

			<p>G2.6 – Gaps on best practice to increment GTP security assessment procedure and on a robust solution against Data session hijacking</p> <p>G2.15 – Gaps on attack surface awareness,</p> <p>G2.17 – Gaps in the design of standards</p>
Interception and unauthorized acquisition (2)	Signalling traffic interception (1)	Core Network, Peering Points	<p>G2.4 – Gaps on the massive deployment of mobile signalling firewalling solutions and anomaly detection systems specific to mobile signalling protocols</p> <p>G2.5 – Gaps in the standardization process to include formal security verification and security assessment/testing of new protocol/network specifications.</p>
	Data session hijacking (2)	Core Network, Peering Points	G2.6 – Gaps on best practice to increment GTP security assessment procedure and on a robust solution against Data session hijacking
	Traffic eavesdropping (3)	Radio Access Network, Infrastructure Network	G2.7 – Gaps on the deployment of the robust crypto algorithm to cipher user plane traffic while minimizing performance impact and interoperability issues
	Traffic redirection (4)	Access Network, Core Network	G2.8 – Gaps on robust and innovative solutions to protect DNS traffic systems.
Nefarious activity/abuse (3)	Exploitation of software bugs (1)	Access Network, Core Network, Infrastructure Network, Endpoint Network	<p>G2.5 – Gaps in the standardization process to include formal security verification and security assessment/testing of new protocol/network specifications</p> <p>G2.16 – Gaps in the security of the new Open Radio Access Network model</p>
	Manipulation of hardware and firmware (2)	Core Network, Access Network, Mobile Edge Computing Infrastructure Network, Endpoint Network	G2.9 – Gaps on wide adoption of integrity-protected firmware also in IoT system

	Malicious code/software/activity (3)	Core Network, Endpoint Network	G2.10 – Gaps on malware detection solution G2.13 – Gaps on the reduced capacity to perform security operations G2.15 – Gaps on attack surface awareness
	Remote activities (execution) (4)	Core Network	G2.2 – Gaps on continuous hardening & patching of IT systems
	Malicious code - Signalling amplification attacks (5)	Access Network, Radio Access Network, Core Network	G2.11 – Gaps on containing amplification attacks
	Exploitation of vulnerabilities in services and remote access infrastructure - COVID-19 (6)	Access Network	G2.2 – Gaps on continuous hardening & patching of IT systems G2.13 – Gaps on the reduced capacity to perform security operations G2.15 – Gaps on attack surface awareness
	Exploitation of System Administrative Tools (7)	Core Network Access Network	G2.14 – Gaps on Defense in Depth G2.15 - Gaps on attack surface awareness G2.16 – Gaps on the security of the new Open Radio Access Network model
	Exploitation of application programming interfaces (APIs) (8)	Core Network Access Network	G2.17 - Gaps in the design of standards
Organization (failure malfunction) (4)	Failures of devices or systems (1)	Access Network, Core Network, Infrastructure Network	G2.1 - Gaps on security testing, on security accreditation schemes of network devices, and on the massive deployment of PSIRT program from vendors
	Supply chain (2)	Infrastructure Network Access Network Core Network	G2.1 - Gaps on security testing, on security accreditation schemes of network devices, and on the massive deployment of PSIRT program from vendors G2.15 - Gaps on attack surface awareness, G2.16 – Gaps on the security of the new Open Radio Access Network model
	Software bug (3)	Access Network, Core Network, Infrastructure Network	G2.1 - Gaps on security testing, on security accreditation schemes of network devices, and on the

			massive deployment of PSIRT program from vendors G2.15: Gaps on attack surface awareness
Intentional Physical Damage (5)	Physical Damage – COVID-19 (1)	Access Network	G2.12 - Gaps on general misinformation campaigns and conspiracy theories

Table 11 provides a binding between identified threats, gaps/challenges, countermeasures, and research actions.

Table 11: Mapping Threats, Gaps, Countermeasures, Research Actions

<b>Threat (T)</b>	<b>Gaps (G)</b>	<b>Countermeasure (C)</b>	<b>Research Action (RA)</b>
T2.1.1 - Erroneous use or administration of devices and systems	G2.2 - Gaps on continuous hardening & patching of IT systems G2.3 – Gaps in security training and awareness toward employees G2.16 - Security of the new Open Radio Access Network model	C2.2 - Automated Patch Management C2.3 - Security by default C2.4 - Adoption of defensive solutions based on AI and ML	RA2.1 - Machine Learning
T2.1.2 - Security misconfigurations in systems/networks	G2.2 – Gaps on continuous hardening & patching of IT systems G2.5 – Gaps in the standardization process to include formal security verification and security assessment/testing of new protocol/network specifications G2.6 – Gaps on best practice to increment GTP security assessment procedure and on a robust solution against Data session hijacking G2.15 – Gaps on attack surface awareness G2.17 – Gaps in the design of standards		RA2.1 - Machine Learning
T2.2.1 - Signalling traffic interception	G2.4 - Gaps on the massive deployment of mobile signalling firewalling solutions and anomaly detection systems specific to mobile signalling protocols G2.5 – Gaps in the standardization process to	C2.5 – Perform periodic network security assessment C2.6 – Implement Monitoring & Event Analysis C2.7 – Adoption of End-to-end security	RA2.2 - Post Quantum security

	include formal security verification and security assessment/testing of new protocol/network specifications.		
T2.2.2 - Data session hijacking	G2.6 – Gaps on best practice to increment GTP security assessment procedure and on a robust solution against Data session hijacking	C2.5 – Perform periodic network security assessment C2.6 – Implement Monitoring & Event Analysis	RA2.1 - Machine Learning
T2.2.3 - Traffic eavesdropping	G2.7 – Gaps on the deployment of the robust crypto algorithm to cipher user plane traffic while minimizing performance impact and interoperability issues	C2.9 - Protection at the network or transport layer with mutual authentication C2.10 – Support and adoption of strong and secure protocols	RA2.2 - Post Quantum security
T2.2.4 - Traffic redirection	G2.8 – Gaps on robust and innovative solutions to protect DNS traffic systems	C2.9 - Protection at the network or transport layer with mutual authentication	RA2.2 - Post Quantum security
T2.3.1 - Exploitation of software bugs	G2.5 – Gaps in the standardization process to include formal security verification and security assessment/testing of new protocol/network specifications G2.16 – Gaps in the security of the new Open Radio Access Network model	C2.8 – Adoption of Formal verification methods in the security protocol design process	RA2.1 - Machine Learning
T2.3.2 - Manipulation of hardware and firmware	G2.9 – Gaps on wide adoption of integrity-protected firmware also in IoT system	C2.14 - Managing firmware updates	RA2.1 - Machine Learning
T2.3.3 - Malicious code/software/activity	G2.10 – Gaps on malware detection solution G2.13 – gaps on the reduced capacity to perform security operations G2.15 – Gaps on attack surface awareness	C2.11 – Threat Intelligence, Integration and Automation C2.4 – Adoption of defensive solutions based on AI and ML	RA2.1 - Machine Learning
T2.3.4 - Remote activities (execution)	G2.2 - Gaps on continuous hardening & patching of IT systems	C2.2 – Automated Patch Management C2.3 – Security by default	RA2.1 - Machine Learning
T2.3.5 - Malicious code - Signalling amplification attacks	G2.11 - Gaps on containing amplification attacks	C2.12 – Adoption of cooperative DDoS attack detection and mitigation	RA2.1 - Machine Learning

T2.3.6 - Exploitation of vulnerabilities in services and remote tools -COVID-19	G2.2 - Gaps on continuous hardening & patching of IT systems G2.13 - Gaps on the reduced capacity to perform security operations G2.15 - Gaps on attack surface awareness	C2.2 – Automated Patch Management C2.3 - Security by default C2.11 - Threat Intelligence, Integration and Automation	RA2.1 - Machine Learning
T2.3.7 - Exploitation of System Administrative Tools	G2.14 - Gaps on Defense in Depth G2.15 - Gaps on attack surface awareness G2.16 - Security of the new Open Radio Access Network model	C2.6 – Monitoring & Event Analysis	RA2.1 - Machine Learning
T2.3.8 - Exploitation of application programming interfaces (APIs)	G2.17 - Gaps in the design of standards	C2.6 – Monitoring & Event Analysis C2.13 – Adoption of enhanced filtering, cross-correlation mechanisms C2.9 - Protection at the network or transport layer with mutual authentication	RA2.1 - Machine Learning
T2.4.1 - Failures of devices or systems	G2.1 - Gaps on security testing, on security accreditation schemes of network devices, and on the massive deployment of PSIRT program from vendors	C2.1 - Vendor Process Evaluation and Product Assurance	RA2.1 - Machine Learning
T2.4.2 -Supply chain	G2.1 - Gaps on security testing, on security accreditation schemes of network devices, and on the massive deployment of PSIRT program from vendors G2.15 - Gaps on attack surface awareness G2.16 - Security of the new Open Radio Access Network model	C2.1 - Vendor Process Evaluation and Product Assurance	RA2.1 - Machine Learning
T2.4.3 - Software bug	G2.1 - Gaps on security testing, on security accreditation schemes of network devices, and on the massive deployment of PSIRT program from vendors G2.15 - Gaps on attack surface awareness	C2.1 - Vendor Process Evaluation and Product Assurance C2.2 – Automated Patch Management C2.5 – Periodic network security assessment	RA2.1 - Machine Learning

T2.5.1 - Physical attack - COVID-19	G2.12 - Gaps on general misinformation campaigns and conspiracy theories		RA2.1 - Machine Learning
-------------------------------------	--	--	--------------------------

### A.3. System-Centric Security

Table 12 presents the complete mapping between assets, threats, and gaps in the System domain using the threat notation of D4.1 (T<domain number>.<threat group number>.<threat number>) and the gap and challenge notation of D4.2 (T<domain number>.<gap number>).

Table 12: Mapping Assets, Threats and Gaps in System Domain

Threat Group (TG)	Threat (T)	Asset (A)	Gaps (G)
Unintentional damage/loss of information or IT assets (1)	Information leakage/sharing due to human errors (1)	Data, Infrastructure	G3.9 - Misconfiguration and inadequate change of control G3.12 - Insider threat, G3.22 – Gaps in user awareness G3.24 - Gaps on the configuration of cloud storage
	Inadequate design and planning or incorrect adaptation (2)	Middleware, Management, Infrastructure	G3.10 - Lack of cloud security architecture and strategy
Interception and unauthorized acquisition (2)	Interception of information (1)	Network, Computer Nodes, Management Server/Console, Access Control/Authorization	G3.3 - Gaps on multi-tenancy, isolation and resource management G3.19 - Race conditions G3.23 - Gaps in network controls
	Unauthorized acquisition of information (data breach) (2)	Data	G3.2 - Gaps in data control G3.3 - Gaps on multi-tenancy, isolation and resource management G3.6 - Gaps in forensics G3.15 - Insecure interfaces and APIs G3.24 - Gaps in the configuration of cloud storage
Poisoning (3)	Configuration poisoning (1)	Middleware, Management, Infrastructure, Security Mechanisms	G3.18 – Malware exposure
	Business process poisoning (2)	Middleware, Management, Infrastructure, Security Mechanisms	G3.18 – Malware exposure
Nefarious activity/abuse (4)	Identity fraud (1)	Middleware, Management, Security Mechanisms	G3.3 - Gaps on multi-tenancy, isolation and resource management

			G3.14 - Abuse and nefarious use of cloud services G3.16 - Account hijacking due to the inadequate authentication
Denial of service (2)	Middleware, Infrastructure, Security Mechanisms		G3.1 - Gaps on the use of cryptography G3.20 - Logistic challenges to the ever-increasing cloud usage
Malicious code/software/activity (3)	Middleware, Security Mechanisms, Virtual File Format		G3.14 - Abuse and nefarious use of cloud services G3.15 - Insecure interfaces and APIs G3.18 – Malware exposure
Generation and use of rogue certificates (4)	Middleware, Management, Infrastructure, Security Mechanisms		G3.7 - Gaps on regulations/standards G3.14 - Abuse and nefarious use of cloud services
Misuse of assurance tools (5)	Data, Middleware, Management, Infrastructure, Security Mechanisms		G3.13 - Weak control planes G3.21 - Gaps on endpoint controls
Failures of the business process (6)	Virtual machine, Platforms, Infrastructure		G3.11 - Insufficient identity, credential, access, and key management G3.17 - Vulnerabilities exposure due to increasing complexity
Code execution and injection (unsecured APIs) (7)	Middleware, Virtual machine, Platforms		G3.15 - Insecure interfaces and APIs
Phishing (8)	Data, Middleware		G3.16 - Account hijacking due to the inadequate authentication
State-sponsored attacks (9)	Data, Infrastructure, Middleware, Management, Security mechanisms		G3.4 – Gaps on roles and human errors G3.5 – Gaps on security assurance and Service Level Agreements (SLA) G3.6 – Gaps on forensics G3.12 – Insider threat G3.14 – Abuse and nefarious use of cloud services G3.15 – Insecure interfaces and APIs G3.17 – Vulnerabilities exposure due to increasing complexity G3.18 – Malware exposure G3.19 – Race conditions G3.23 – Gaps on remote network controls

Legal (5)	Violation of laws or regulations (1)	All assets.	G3.5 - Gaps on security assurance and Service Level Agreements (SLAs) G3.7 - Gaps on regulations/standards
Organizational threats (6)	Skill shortage (1)	Roles	G3.4 - Gaps on roles and human resources G3.9 - Misconfiguration and inadequate change of control G3.13 - Weak control planes G3.24 - Gaps in the configuration of cloud storage
	Malicious insider (2)	Data, Middleware, Management, Infrastructure, Security Mechanisms	G3.12 - Insider threat G3.16 - Account hijacking due to the inadequate authentication
	The lack of awareness (3)	Roles	G3.9 - Misconfiguration and inadequate change of control G3.10 - Lack of cloud security architecture and strategy G3.12 - Insider threat G3.22 - Gaps on user awareness G3.24 - Gaps on the configuration of cloud storage
	<i>Personal cloud service adoption– COVID-19(4)</i>	Management, Security Mechanisms, Middleware	G3.21 - Gaps on endpoint controls
	Cloud sprawl (5)	Roles	G3.10 - Lack of cloud security architecture and strategy G3.22 – Gaps on user awareness

Table 13 provides a binding between identified threats, gaps/challenges, countermeasures, and research actions.

Table 13: Mapping Threats, Gaps, Countermeasures, Research Actions

Threat (T)	Gap (G)	Countermeasure (C)	Research Action (RA)
T3.1.1 - Information leakage/sharing due to human errors	G3.9 - Misconfiguration and inadequate change of control G3.12 - Insider threat G3.22 – Gaps on user awareness G3.24 - Gaps on the configuration of cloud storage	C3.9 - Raising security awareness	RA3.4 - Cloud-to-cloud backup
T3.1.2 - Inadequate design and planning or incorrect adaptation	G3.10 - Lack of cloud security architecture and strategy	C3.8 - Making systems secure by default C3.9 - Raising security awareness	RA3.1 – SDN RA3.2 - ML/AI-based solutions
T3.2.1 - Interception of information	G3.3 - Gaps on multi-tenancy, isolation and resource management G3.19 - Race conditions G3.23 - Gaps on network controls	C3.2 - Encryption and key management C3.3 - Virtual trusted platform module (vTPM) and trusted virtual domains (TVDs) C3.4 - Enforcing access control mechanisms (ACMs)	RA3.2 - ML/AI-based solutions RA3.3 - Data encryption
T3.2.2 - Unauthorized acquisition of information (data breach)	G3.2 - Gaps on data control G3.3 - Gaps on multi-tenancy, isolation, and resource management G3.6 - Gaps on forensics G3.15 - Insecure interfaces and APIs G3.24 - Gaps on the configuration of cloud storage	C3.2 - Encryption and key management C3.3 - Virtual trusted platform module (vTPM) and trusted virtual domains (TVDs) C3.4 - Enforcing access control mechanisms (ACMs)	RA3.2 - ML/AI-based solutions RA3.3 - Data encryption RA3.4 - Cloud-to-cloud backup
T3.3.1 - Configuration poisoning	G3.18 – Malware exposure	C3.5 - Maintaining proper configuration of virtualized and cloud environments	RA3.2 - ML/AI-based solutions
T3.3.2 - Business process poisoning	G3.18 – Malware exposure	C3.6 - Isolating guest operating systems	RA3.2 - ML/AI-based solutions RA3.3 - Data encryption

T3.4.1 - Identity fraud	G3.3 - Gaps on multi-tenancy, isolation, and resource management G3.14 - Abuse and nefarious use of cloud services G3.16 - Account hijacking due to the inadequate authentication	C3.2 - Encryption and key management C3.4 - Enforcing access control mechanisms (ACMs)	RA3.3 - Data encryption
T3.4.2 - Denial of service	G3.1 - Gaps in the use of cryptography G3.20 - Logistic challenges to the ever-increasing cloud usage	C3.5 - Maintaining proper configuration of virtualized and cloud environments C3.7 - Monitoring and maintaining hypervisor/VMM activities	RA3.4 - Cloud-to-cloud backup
T3.4.3 - Malicious code/software/activity	G3.14 - Abuse and nefarious use of cloud services G3.15 - Insecure interfaces and APIs G3.18 - Malware exposure	C3.1 - Firewalls C3.3 - Virtual trusted platform module (vTPM) and trusted virtual domains (TVDs) C3.7 - Monitoring and maintaining hypervisor/VMM activities C3.8 - Making systems secure by default	RA3.1 - SDN RA3.2 - ML/AI-based solutions
T3.4.4 - Generation and use of rogue certificates	G3.7 - Gaps in regulations/standards G3.14 - Abuse and nefarious use of cloud services	C3.3 - Virtual trusted platform module (vTPM) and trusted virtual domains (TVDs) C3.7 - Monitoring and maintaining hypervisor/VMM activities	RA3.1 - SDN
T3.4.5 - Misuse of assurance tools	G3.13 - Weak control planes, G3.21 - Gaps on endpoint controls	C3.8 - Making systems secure by default, C3.10- Enforcing regulations	
T3.4.6 - Failures of business processes	G3.11 - Insufficient identity, credential, access, and key management G3.17 - Vulnerabilities exposure due to increasing complexity	C3.8 - Making systems secure by default C3.9 - Raising security awareness	RA3.1 - SDN RA3.2 - ML/AI-based solutions RA3.4 - Cloud-to-cloud backup
T3.4.7 - Code execution and	G3.15 - Insecure interfaces and APIs	C3.1 - Firewalls, C3.7 - Monitoring and maintaining	RA3.1 - SDN RA3.2 - ML/AI-based solutions

injection (unsecured APIs)		hypervisor/VMM activities	
T3.4.8 - Phishing - COVID-19	G3.16 - Account hijacking due to the inadequate authentication	C3.1 - Firewalls C3.9 - Raising security awareness	RA3.2 - ML/AI-based solutions
T3.4.9 – State-sponsored attacks	G3.4 – Gaps on roles and human errors G3.5 – Gaps on security assurance and Service Level Agreements (SLA) G3.6 – Gaps on forensics G3.12 – Insider threat G3.14 – Abuse and nefarious use of cloud services G3.15 – Insecure interfaces and APIs G3.17 – Vulnerabilities exposure due to increasing complexity G3.18 – Malware exposure G3.19 – Race conditions G3.23 – Gaps on remote network controls	C3.1 - Firewalls C3.4 – Enforcing Access Control Mechanisms C3.5 - Maintaining proper configuration of virtualized and cloud environments C3.6 – Isolating guest operating systems C3.7 – Monitoring and maintaining hypervisor/VMM activities C3.8 – Making systems secure by default C3.9 – Raising security awareness	RA3.2 - ML/AI-based solutions RA3.4 – Cloud-to-cloud backup
T3.5.1 - Violation of laws or regulations	G3.5 - Gaps on security assurance and Service Level Agreements (SLAs) G3.7 - Gaps on regulations/standards	C3.10 - Enforcing regulations	RA3.1 – SDN RA3.2 - ML/AI-based solutions
T3.6.1 - Skill shortage	G3.4 - Gaps on roles and human resources G3.9 - Misconfiguration and inadequate change of control G3.13 - Weak control planes G3.24 - Gaps in the configuration of cloud storage	C3.9 - Raising security awareness	
T3.6.2 - Malicious insider	G3.12 - Insider threat G3.16 - Account hijacking due to the inadequate authentication	C3.3 - Virtual trusted platform module (vTPM) and trusted virtual domains (TVDs) C3.4 - Enforcing access control mechanisms (ACMs) C3.7 - Monitoring and maintaining	RA3.1 – SDN RA3.4 - Cloud-to-cloud backup

		hypervisor/VMM activities	
T3.6.3 - The lack of awareness	G3.9 - Misconfiguration and inadequate change of control G3.10 - Lack of cloud security architecture and strategy G3.12 - Insider threat G3.22 - Gaps on user awareness G3.24 - Gaps on the configuration of cloud storage	C3.9 - Raising security awareness	
T3.6.4 - Personal cloud service adoption - COVID-19	G3.21 - Gaps on endpoint controls	C3.9 - Raising security awareness	
T3.6.5 – Cloud sprawl - COVID-19	G3.10 - Lack of cloud security architecture and strategy G3.22 – Gaps on user awareness	C3.9 - Raising security awareness	RA3.1 – SDN RA3.2 - ML/AI-based solutions

**A.4. Data-Centric Security**

Table 14 presents the complete mapping between assets, threats, and gaps in the Data domain using the threat notation of D4.1 (T<domain number>.<threat group number>.<threat number>) and the gap and challenge notation of D4.2 (T<domain number>.<gap number>).

Table 14: Mapping Assets, Threats and Gaps in Data Domain

Threat Group (TG)	Threat (T)	Asset (A)	Gaps (G)
Unintentional damage/loss of information or IT assets (1)	Information leakage/sharing due to human errors (1)	Data, Infrastructure	G4.1 - Gaps in data protection G4.4 - Gaps in roles (skill shortage) G4.8 - Gaps in videoconferencing tools G4.9 - Gaps in data management across borders
	Inadequate design and planning or incorrect adaptation (2)	Data, Big Data analytics, Software, Computing Infrastructure models, Storage Infrastructure models	G4.1 - Gaps in data protection G4.2 - Gaps in the use of cryptography in applications and back-end services G4.3 - Gaps in computing and storage models and infrastructures G4.4 - Gaps in roles (skill shortage)
	Information leakage/sharing due to the hostile home network - COVID-19 (3)	Data, Infrastructure	G4.1 - Gaps in data protection G4.4 - Gaps in roles (skill shortage) G4.8 - Gaps in videoconferencing tools

			G4.9 - Gaps in data management across borders
Interception and unauthorized acquisition (2)	Interception of information (1)	Data, Roles, Infrastructure	G4.1 - Gaps in data protection G4.2 - Gaps in the use of cryptography in applications and back-end services G4.3 - Gaps in computing and storage models and infrastructures G4.4 - Gaps in roles (skill shortage) G4.9 - Gaps on data management across borders G4.10 - Gaps in the distributed data and frameworks
	Unauthorized acquisition of information (data breach) (2)	Data, Roles, Infrastructure	G4.1 - Gaps in data protection G4.2 - Gaps in the use of cryptography in applications and back-end services G4.3 - Gaps in computing and storage models and infrastructures G4.4 - Gaps in roles (skill shortage) G4.8 - Gaps in videoconferencing tools G4.9 - Gaps on data management across borders G4.11 – Gaps in the use of non-relational databases
	Conversation Eavesdropping/Hijacking - COVID-19 (3)	Data, Roles, Data privacy	G4.1 - Gaps in data protection G4.2 - Gaps in the use of cryptography in applications and back-end services G4.7 - Gaps on ethics G4.8 - Gaps in videoconferencing tools
Poisoning (3)	Data poisoning (1)	Data, Security and privacy techniques, Data management, Data privacy.	G4.1 - Gaps on data protection G4.4 - Gaps on roles (skill shortage) G4.5 - Gaps on data trustworthiness G4.6 - Gaps on decision support systems G4.11 – Gaps on the use of non-relational databases
	Model poisoning (2)	Data, Data Analytics	G4.1 - Gaps on data protection G4.4 - Gaps on roles (skill shortage) G4.5 - Gaps on data trustworthiness

			G4.6 - Gaps on decision support systems
	Unreliable data (3)	Data, Big Data analytics, Data privacy	G4.1 - Gaps on data protection G4.2 - Gaps on the use of cryptography in applications and back-end services G4.3 - Gaps on computing and storage models and infrastructures G4.5 - Gaps on data trustworthiness G4.11 – Gaps on the use of non-relational databases
Nefarious activity/abuse (4)	Identity fraud (1)	Data, Infrastructure	G4.1 - Gaps on data protection G4.5 - Gaps on data trustworthiness G4.7 - Gaps on ethics G4.9 - Gaps on data management across borders
	Denial of service (2)	Infrastructure	G4.1 - Gaps on data protection G4.2 - Gaps on the use of cryptography in applications and back-end services G4.3 - Gaps on computing and storage models and infrastructures
	Malicious code/software/activity (3)	Data, Software, Computing infrastructure models	G4.1 - Gaps on data protection G4.2 - Gaps on the use of cryptography in applications and back-end services G4.3 - Gaps on computing and storage models and infrastructures G4.9 - Gaps on data management across borders G4.10 - Gaps on the distributed data and frameworks G4.11 – Gaps on the use of non-relational databases
	Generation and use of rogue certificates (4)	Data, Big Data analytics, Software, Hardware	G4.1 - Gaps on data protection G4.2 - Gaps on the use of cryptography in applications and back-end services
	Misuse of assurance tools (5)	Security and Privacy Techniques, Data, Infrastructure	G4.1 - Gaps on data protection G4.5 - Gaps on data trustworthiness G4.6 - Gaps on decision support systems

	Failures of business process (6)	Data, Big Data analytics	G4.1 - Gaps on data protection G4.4 - Gaps on roles (skill shortage) G4.6 - Gaps on decision support systems
	Code execution and injection (unsecured APIs) (7)	Data, Storage Infrastructure models	G4.1 - Gaps on data protection G4.2 - Gaps on the use of cryptography in applications and back-end services G4.3 - Gaps on computing and storage models and infrastructures G4.9 - Gaps on data management across borders
	Data extraction from ML models (8)	Data, Data analytics	G4.1 - Gaps on data protection G4.3 - Gaps on computing and storage models and infrastructures G4.7 - Gaps on ethics
	Extortion attacks (9)	Data, Security and privacy techniques	G4.1 - Gaps on data protection G4.2 - Gaps on the use of cryptography in applications and back-end services
Legal (5)	Violation of laws or regulations (1)	All assets.	G4.1 - Gaps on data protection G4.7 - Gaps on ethics
Organizational threats (6)	Skill shortage (1)	Roles	G4.1 - Gaps on data protection G4.4 - Gaps on roles (skill shortage)
	Malicious insider (2)	Roles, Data, Infrastructure Security, Integrity and Reactive Security	G4.1 - Gaps on data protection G4.4 - Gaps on roles (skill shortage) G4.7 - Gaps on ethics

Table 15 provides a binding between identified threats, gaps/challenges, countermeasures, and research actions.

Table 15: Mapping Threats, Gaps, Countermeasures, Research Actions

Threat (T)	Gap (G)	Countermeasure (C)	Research Action (RA)
T4.1.1 - Information leakage/sharing due to human errors	G4.1 - Gaps on data protection G4.4 - Gaps on roles (skill shortage) G4.8 - Gaps in videoconferencing tools	C4.5 - Enforcing password hygiene C4.8 - User awareness training and education	RA4.2 - Access control and data encryption RA4.4 - Self-destructing data

	G4.9 - Gaps on data management across borders		
T4.1.2 - Inadequate design and planning or incorrect adaptation	G4.1 - Gaps on data protection G4.2 - Gaps on the use of cryptography in applications and back-end services G4.3 - Gaps on computing and storage models and infrastructures G4.4 - Gaps on roles (skill shortage)	C4.8 - User awareness training and education	RA4.1 - Decentralized and blockchain-based solutions
T4.1.3 - Information leakage/sharing due to the hostile home network - COVID-19	G4.1 - Gaps on data protection G4.4 - Gaps on roles (skill shortage) G4.8 - Gaps in videoconferencing tools G4.9 - Gaps on data management across borders	C4.5 - Enforcing password hygiene C4.8 - User awareness training and education	RA4.2 - Access control and data encryption RA4.4 - Self-destructing data
T4.2.1 - Interception of information	G4.1 - Gaps on data protection G4.2 - Gaps on the use of cryptography in applications and back-end services G4.3 - Gaps on computing and storage models and infrastructures G4.4 - Gaps on roles (skill shortage) G4.9 - Gaps on data management across borders G4.10 - Gaps on the distributed data and frameworks	C4.3 - Anti-malware, antivirus, and endpoint protection C4.4 - Data security auditing C4.7 - Deployment of intrusion detection and prevention systems	RA4.2 - Access control and data encryption RA4.3 - ML/AI-based solutions
T4.2.2 - Unauthorized acquisition of information (data breach)	G4.1 - Gaps on data protection G4.2 - Gaps on the use of cryptography in applications and back-end services G4.3 - Gaps on computing and storage models and infrastructures G4.4 - Gaps on roles (skill shortage) G4.8 - Gaps in videoconferencing tools G4.9 - Gaps on data management across borders G4.11 – Gaps on the use of non-relational databases	C4.1 - Identity access management C4.2 - Data masking and encryption C4.3 - Anti-malware, antivirus, and endpoint protection C4.5 - Enforcing password hygiene C4.7 - Deployment of intrusion detection and prevention systems	RA4.1 - Decentralized and blockchain-based solutions RA4.2 - Access control and data encryption RA4.3 - ML/AI-based solutions RA4.4 - Self-destructing data
T4.2.3 - Conversation	G4.1 - Gaps on data protection		RA4.1 - Decentralized and

Eavesdropping/ Hijacking - COVID-19	G4.2 - Gaps on the use of cryptography in applications and back-end services G4.7 - Gaps on ethics G4.8 - Gaps in videoconferencing tools		blockchain-based solutions RA4.2 - Access control and data encryption RA4.3 - ML/AI-based solutions
T4.3.1 - Data poisoning	G4.1 - Gaps on data protection G4.4 - Gaps on roles (skill shortage) G4.5 - Gaps on data trustworthiness G4.6 - Gaps on decision support systems G4.11 – Gaps on the use of non-relational databases	C4.1 - Identity access management C4.2 - Data masking and encryption C4.9 – Data poisoning detection	RA4.3 - ML/AI-based solutions
T4.3.2 - Model poisoning	G4.1 - Gaps on data protection G4.4 - Gaps on roles (skill shortage) G4.5 - Gaps on data trustworthiness G4.6 - Gaps on decision support systems	C4.1 - Identity access management C4.2 - Data masking and encryption C4.9 – Data poisoning detection	RA4.3 - ML/AI-based solutions
T4.3.3 - Unreliable data	G4.1 - Gaps on data protection G4.2 - Gaps on the use of cryptography in applications and back-end services G4.3 - Gaps on computing and storage models and infrastructures G4.5 - Gaps on data trustworthiness G4.11 – Gaps on the use of non-relational databases		RA4.4 - Self-destructing data
T4.4.1 - Identity fraud	G4.1 - Gaps on data protection G4.5 - Gaps on data trustworthiness G4.7 - Gaps on ethics G4.9 - Gaps on data management across borders	C4.1 - Identity access management C4.5 - Enforcing password hygiene C4.8 - User awareness training and education	RA4.2 - Access control and data encryption
T4.4.2 - Denial of service	G4.1 - Gaps on data protection G4.2 - Gaps on the use of cryptography in applications and back-end services G4.3 - Gaps on computing and storage models and infrastructures	C4.4 - Data security auditing, C4.6 - Data backups C4.7 - Deployment of intrusion detection and prevention systems	RA4.1 - Decentralized and blockchain-based solutions

T4.4.3 - Malicious code/software/activity	G4.1 - Gaps on data protection G4.2 - Gaps on the use of cryptography in applications and back-end services G4.3 - Gaps on computing and storage models and infrastructures G4.9 - Gaps on data management across borders G4.10 - Gaps on the distributed data and frameworks G4.11 – Gaps on the use of non-relational databases	C4.3 - Anti-malware, antivirus, and endpoint protection C4.4 - Data security auditing C4.6 - Data backups C4.7 - Deployment of intrusion detection and prevention systems	RA4.3 - ML/AI-based solutions RA4.4 - Self-destructing data
T4.4.4 - Generation and use of rogue certificates	G4.1 - Gaps on data protection G4.2 - Gaps on the use of cryptography in applications and back-end services	C4.1 - Identity access management C4.7 – Deployment of intrusion detection and prevention systems	
T4.4.5 - Misuse of assurance tools	G4.1 - Gaps on data protection G4.5 - Gaps on data trustworthiness G4.6 - Gaps on decision support systems	C4.1 - Identity access management C4.7 - Deployment of intrusion detection and prevention systems	RA4.3 - ML/AI-based solutions
T4.4.6 - Failures of business processes	G4.1 - Gaps on data protection G4.4 - Gaps on roles (skill shortage) G4.6 - Gaps on decision support systems	C4.1 - Identity access management C4.2 - Data masking and encryption C4.4 - Data security auditing C4.6 - Data backups	RA4.1 - Decentralized and blockchain-based solutions RA4.3 - ML/AI-based solutions
T4.4.7 - Code execution and injection (unsecured APIs)	G4.1 - Gaps on data protection G4.2 - Gaps on the use of cryptography in applications and back-end services G4.3 - Gaps on computing and storage models and infrastructures G4.9 - Gaps on data management across borders	C4.3 - Anti-malware, antivirus, and endpoint protection C4.4 - Data security auditing C4.7 - Deployment of intrusion detection and prevention systems	RA4.3 - ML/AI-based solutions
T4.4.8 – Data extraction from ML models	G4.1 - Gaps on data protection G4.3 – Gaps on computing and storage models and infrastructures G4.7 – Gaps on ethics	C4. 2 – Data masking and encryption C4.7 - Deployment of intrusion detection and prevention systems	RA4.3 – ML/AI-based solutions
T4.4.9 – Extortion attacks	G4.1 - Gaps on data protection G4.2 - Gaps on the use of cryptography in applications and back-end services	C4.1 – Identity Access Management C4. 2 – Data masking and encryption	RA4.2 – Access control and data encryption RA4.3 – ML/AI-based solutions

		C4.3 – Anti-malware, antivirus, and endpoint protection C4.4 – Data security auditing C4.8 – User awareness training and education C4.7 - Deployment of intrusion detection and prevention systems	RA4,4 – Self-destructing data
T4.5.1 - Violation of laws or regulations	G4.1 - Gaps on data protection G4.7 - Gaps on ethics	C4.1 - Identity access management C4.8 - User awareness training and education	RA4.1 - Decentralized and blockchain-based solutions
T4.6.1 - Skill shortage	G4.1 - Gaps on data protection G4.4 - Gaps on roles (skill shortage)	C4.8 - User awareness training and education	RA4.1 - Decentralized and blockchain-based solutions
T4.6.2 - Malicious insider	G4.1 - Gaps on data protection G4.4 - Gaps on roles (skill shortage) G4.7 - Gaps on ethics	C4.1 - Identity access management C4.2 - Data masking and encryption	RA4.4 - Self-destructing data

### A.5. Application-Centric Security

Table 16 presents the complete mapping between assets, threats, and gaps in the Application domain using the threat notation of D4.1 (T<domain number>.<threat group number>.<threat number>) and the gap and challenge notation of D4.2 (T<domain number>.<gap number>).

Table 16 Mapping Assets, Threats and Gaps in Application Domain

Threat Group (TG)	Threat (T)	Asset (A)	Gaps (G)
Unintentional damage (1)	Security misconfiguration (1)	Interfaces, Security Techniques	G5.1 - Gaps on microservice-aware security G5.2 - Gaps on authentication and authorization G5.3 - Gaps on orchestration and composition G5.5 - Gaps on the proper management of configurations G5.7 - Gaps on skills
	Inadequate design (2)	All	G5.2 - Gaps on authentication and authorization G5.3 - Gaps on orchestration and composition G5.7 - Gaps on skills G5.8 - Gaps on interoperability
Interception and unauthorized acquisition (2)	Interception of information (1)	Data, Interfaces, Security Techniques	G5.1 - Gaps on microservice-aware security G5.2 - Gaps on authentication and authorization G5.3 - Gaps on orchestration and composition G5.7 - Gaps on skills
	Sensitive data exposure (2)	Data, Security Techniques, Roles	G5.1 - Gaps on microservice-aware security G5.2 - Gaps on authentication and authorization G5.3 - Gaps on orchestration and composition G5.4 - Gaps on safety and security by default G5.5 - Gaps on the proper management of configurations G5.7 - Gaps on skills
Nefarious activity/abuse (3)	Broken authentication and access control (1)	Data, Security Techniques, Roles	G5.1 - Gaps on microservice-aware security G5.2 - Gaps on authentication and authorization

			G5.3 - Gaps on orchestration and composition G5.4 - Gaps on safety and security by default G5.7 - Gaps on skills
	Denial of service (2)	Data, Interfaces, Security Techniques, Roles	G5.3 - Gaps on orchestration and composition G5.4 - Gaps on safety and security by default G5.7 - Gaps on skills G5.10 - Gaps on sophisticated protection
	Code execution and injection (unsecured APIs) (3)	Data, Interfaces, Security Techniques	G5.1 - Gaps on microservice-aware security G5.4 - Gaps on safety and security by default G5.7 - Gaps on skills
	Insufficient logging and monitoring (4)	Data, Interfaces, Security Techniques	G5.3 - Gaps on orchestration and composition G5.4 - Gaps on safety and security by default G5.7 - Gaps on skills
	Untrusted composition (5)	Interfaces	G5.3 - Gaps on orchestration and composition G5.4 - Gaps on safety and security by default G5.7 - Gaps on skills
	Supply-chain security (6)	All	G5.6 - Gaps on supply-chain security
	Virtualization (7)	Data, Interfaces	G5.3 - Gaps on orchestration and composition G5.6 - Gaps on supply-chain security
	Source code breach (8)	Data, Interfaces, Security techniques	G5.5 – Gaps on the proper management of configurations G5.6 – Gaps on supply-chain security G5.7 – Gaps on skills G5.10 – Gaps on sophisticated protection
Legal (4)	Violations of laws or regulations (1)	All	G5.7 - Gaps on skills G5.9 - Gaps on education
Organizational threats (5)	Malicious insider (1)	Application Security, Data, Platform Security, Roles	G5.9 - Gaps on education G5.10 - Gaps on sophisticated protection
	Skill shortage (2)	All	G5.7 - Gaps on skills G5.9 - Gaps on education

Table 17 provides a binding between identified threats, gaps/challenges, countermeasures, and research actions.

Table 17: Mapping Threats, Gaps, Countermeasures, Research Actions

<b>Threat (T)</b>	<b>Gap (G)</b>	<b>Countermeasure (C)</b>	<b>Research Action (R)</b>
T5.1.1 - Security misconfiguration	G5.1 - Gaps on microservice-aware security G5.2 - Gaps on authentication and authorization G5.3 - Gaps on orchestration and composition G5.5 - Gaps on the proper management of configurations G5.7 - Gaps on skills	C5.1 - Security by default C5.3 - Orchestration Platforms C5.4 - Sandboxing	RA5.1 - Zero Trust Security
T5.1.2 - Inadequate design	G5.2 - Gaps on authentication and authorization G5.3 - Gaps on orchestration and composition G5.7 - Gaps on skills G5.8 - Gaps on interoperability	C5.2 - Authentication and Authorization C5.3 - Orchestration Platforms C5.4 - Sandboxing	RA5.1 - Zero Trust Security RA5.2 - AI/ML for Security RA5.3 - Authentication RA5.4 - Supply - Chain
T5.2.1 - Interception of information	G5.1 - Gaps on microservice-aware security G5.2 - Gaps on authentication and authorization G5.3 - Gaps on orchestration and composition G5.7 - Gaps on skills	C5.1 - Security by default C5.3 - Orchestration Platforms	RA5.1 - Zero Trust Security RA5.2 - AI/ML for Security
T5.2.2 - Sensitive data exposure	G5.1 - Gaps on microservice-aware security G5.2 - Gaps on authentication and authorization G5.3 - Gaps on orchestration and composition G5.4 - Gaps on safety and security by default G5.5 - Gaps on the proper management of configurations	C5.1 - Security by default C5.2 - Authentication and Authorization C5.3 - Orchestration Platforms	RA5.1 - Zero Trust Security RA5.3 - Authentication RA5.4 - Supply -Chain

	G5.7 - Gaps on skills		
T5.3.1 - Broken authentication and access control	G5.1 - Gaps on microservice-aware security G5.2 - Gaps on authentication and authorization G5.3 - Gaps on orchestration and composition G5.4 - Gaps on safety and security by default G5.7 - Gaps on skills	C5.1 - Security by default C5.2 - Authentication and Authorization C5.3 - Orchestration Platforms	RA5.1 - Zero Trust Security, RA5.3 – Authentication RA5.4 - Supply -Chain
T5.3.2 - Denial of service	G5.3 - Gaps on orchestration and composition G5.4 - Gaps on safety and security by default G5.7 - Gaps on skills G5.10 - Gaps on sophisticated protection	C5.3 - Orchestration Platforms	RA5.1 - Zero Trust Security RA5.2 - AI/ML for Security
T5.3.3 - Code execution and injection (unsecured APIs)	G5.1 - Gaps on microservice-aware security G5.4 - Gaps on safety and security by default G5.7 - Gaps on skills	C5.1 - Security by default C5.3 - Orchestration Platforms C5.4 - Sandboxing	RA5.1 - Zero Trust Security RA5.4 – Supply -Chain
T5.3.4 - Insufficient logging and monitoring	G5.3 - Gaps on orchestration and composition G5.4 - Gaps on safety and security by default G5.7 - Gaps on skills	C5.3 - Orchestration Platforms	
T5.3.5 - Untrusted composition	G5.3 - Gaps on orchestration and composition G5.4 - Gaps on safety, and security by default G5.7 - Gaps on skills	C5.3 - Orchestration Platforms	RA5.1 - Zero Trust Security RA5.4 - Supply -Chain
T5.3.6 - Supply-chain security	G5.6 - Gaps on supply-chain security	C5.1 - Security by default	RA5.1 - Zero Trust Security RA5.2 - AI/ML for Security RA5.4 - Supply -Chain
T5.3.7 - Virtualization	G5.3 - Gaps on orchestration and composition	C5.3 - Orchestration Platforms C5.4 - Sandboxing	RA5.4 - Supply -Chain

	G5.6 - Gaps on supply-chain security		
T5.3.8 – Source code breach	G5.5 – Gaps on the proper management of configurations G5.6 – Gaps on supply-chain security G5.7 – Gaps on skills G5.10 – Gaps on sophisticated protection	C5.1 - Security by default C5.4 - Sandboxing	RA5.3 - Authentication RA5.4 – Supply-chain
T5.4.1 - Violations of laws or regulations	G5.7 - Gaps on skills G5.9 - Gaps on education		
T5.5.1 - Malicious insider	G5.9 - Gaps on education G5.10 - Gaps on sophisticated protection	C5.2 - Authentication and Authorization	RA5.2 - AI/ML for Security
T5.5.2 - Skill shortage	G5.7 - Gaps on skills G5.9 - Gaps on education		

We note that threats T5.5.2 – Skill Shortage and T5.4.1 – Violations and laws or regulations are horizontal to all countermeasures and research actions, and therefore the mapping in the table is empty.

### A.6. User-Centric Security

Table 18 presents the complete mapping between assets, threats, and gaps in the User domain using the threat notation of D4.1 (T<domain number>.<threat group number>.<threat number>) and the gap and challenge notation of D4.2 (T<domain number>.<gap number>).

Table 18: Mapping Assets, Threats and Gaps in User Domain

Threat Group (TG)	Threat (T)	Asset (A)	Gaps (G)
Human errors (1)	Mishandling of physical assets (1)	All assets.	G6.4 – Gaps on security training and education
	Misconfiguration of systems (2)	All assets.	G6.4 – Gaps on security training and education
	Loss of CIA on data assets (3)	All assets.	G6.1 – Gaps on modelling user behavior G6.2 – Gaps on the relation between user behavior and adverse security-related effects G6.4 – Gaps on

			security training and education
	Legal, reputational, and financial cost (4)	All assets.	G6.3 – Gaps on security information G6.5 – Gaps in collaborative protocols for disclosure
Privacy breaches (2)	Profiling and discriminatory practices (1)	External	G6.5 – Gaps in collaborative protocols for disclosure G6.6 - Gaps on protection from online scammers
	Illegal acquisition of information (2)	All assets.	G6.1 – Gaps on modelling user behavior G6.2 – Gaps on the relation between user behavior and adverse security-related effects G6.4 – Gaps on security training and education
Cybercrime (3)	Organized criminal groups' activity (1)	Internal, Intangible	G6.1 – Gaps on modelling user behavior G6.2 – Gaps on the relation between user behavior and adverse security-related effects G6.4 – Gaps on security training and education
	State-sponsored organizations' activity (2)	All assets.	G6.1 – Gaps on modelling user behavior G6.2 – Gaps on the relation between user behavior and adverse security-related effects
	Malicious employees or partners' activity (3)	Internal	G6.1 – Gaps on modelling user behavior G6.2 – Gaps on the relation between user behavior and adverse security-related effects G6.5 – Gaps in collaborative protocols for disclosure

Media amplification effects (4)	Misinformation/disinformation campaigns (1)	All assets.	G6.3 – Gaps on security information G6.4 – Gaps on security training and education G6.6 - Gaps on protection from online scammers
	Smear campaigns/market manipulation (2)	All assets.	G6.3 – Gaps on security information G6.4 – Gaps on security training and education G6.6 - Gaps on protection from online scammers
	Social responsibility/ethics-related accidents (3)	All assets.	G6.3 – Gaps on security information G6.4 – Gaps on security training and education G6.6 - Gaps on protection from online scammers
Organizational threats (5)	Skill shortage/undefined cybersecurity curricula (1)	Internal	G6.4 – Gaps on security training and education G6.6 - Gaps on protection from online scammers
	Business misalignment/shift of priorities (2)	Internal, External	G6.5 – Gaps in collaborative protocols for disclosure
	Pivoting (3)	All assets.	G6.1 – Gaps on modelling user behavior G6.2 – Gaps on the relation between user behavior and adverse security-related effects G6.4 – Gaps on security training and education

Table 19 provides a binding between identified threats, gaps/challenges, countermeasures, and research actions.

Table 19: Mapping Threats, Gaps, Countermeasures, Research Actions

Threat (T)	Gap (G)	Countermeasure (C)	Research Action (RA)
T6.1.1 - Mishandling of physical assets	G6.4 – Gaps on security training and education	C6.1 – Security training C6.3 – Data encryption C6.6 – Multi-factor authentication	RA6.1 – Security training techniques
T6.1.2 - Misconfiguration of systems	G6.4 – Gaps on security training and education	C6.1 – Security training C6.2 – Assessment of security standards implementation C6.11 – Code analysis	RA6.1 – Security training techniques RA6.4 – AI applications for user security
T6.1.3 - Loss of CIA on data assets	G6.1 – Gaps on modelling user behavior G6.2 – Gaps on the relation between user behavior and adverse security-related effects G6.4 – Gaps on security training and education	C6.1 – Security training C6.3 – Data encryption C6.4 – Access control policies C6.9 – Tokens leaks prevention and mitigation	RA6.1 – Security training techniques RA6.3 – Social engineering and user behavior RA6.4 – AI applications for user security
T6.1.4 - Legal, reputational, and financial cost	G6.3 – Gaps on security information G6.5 – Gaps in collaborative protocols for disclosure	C6.12 – Legal audit	RA6.3 – Social engineering and user behavior
T6.2.1 - Profiling and discriminatory practices	G6.5 – Gaps in collaborative protocols for disclosure G6.6 - Gaps on protection from online scammers	C6.3 – Data encryption C6.12 – Legal audit	RA6.2 – Fight against disinformation
T6.2.2 - Illegal acquisition of information	G6.1 – Gaps on modelling user behavior G6.2 – Gaps on the relation between user behavior and adverse security-related effects G6.4 – Gaps on security training and education	C6.1 – Security training C6.3 – Data encryption C6.4 – Access control policies C6.9 – Tokens leaks prevention and mitigation	RA6.1 – Security training techniques RA6.3 – Social engineering and user behavior RA6.4 – AI applications for user security
T6.3.1 - Organized criminal groups' activity	G6.1 – Gaps on modelling user behavior	C6.1 – Security training C6.3 – Data encryption	RA6.3 – Social engineering and user behavior RA6.4 – AI

	G6.2 – Gaps on the relation between user behavior and adverse security-related effects G6.4 – Gaps on security training and education	C6.6 – Multi-factor authentication C6.7 – Firewall C6.8 – Traffic analysis C6.10 – Log analysis C6.13 – Honeypots	applications for user security
T6.3.2 - State-sponsored organizations' activity	G6.1 – Gaps on modelling user behavior G6.2 – Gaps on the relation between user behavior and adverse security-related effects	C6.7 – Firewall C6.8 – Traffic analysis	RA6.3 – Social engineering and user behavior RA6.4 – AI applications for user security
T6.3.3 - Malicious employees or partners' activity	G6.1 – Gaps on modelling user behavior G6.2 – Gaps on the relation between user behavior and adverse security-related effects G6.5 – Gaps in collaborative protocols for disclosure	C6.4 – Access control policies C6.10 – Log analysis C6.12 – Legal audit	RA6.3 – Social engineering and user behavior
T6.4.1 - Misinformation/disinformation campaigns	G6.3 – Gaps on security information G6.4 – Gaps on security training and education G6.6 - Gaps on protection from online scammers	C6.1 – Security training C6.5 - Increase awareness on security and technology use	RA6.2 – Fight against disinformation
T6.4.2 - Smear campaigns/market manipulation	G6.3 – Gaps on security information G6.4 – Gaps on security training and education G6.6 - Gaps on protection from online scammers	C6.2 – Assessment of security standards implementation C6.5 - Increase awareness on security and technology use C6.12 – Legal audit	RA6.2 – Fight against disinformation
T6.4.3 - Social responsibility/ethics-related accidents	G6.3 – Gaps on security information G6.4 – Gaps on security training and education G6.6 - Gaps on protection from online scammers	C6.5 - Increase awareness on security and technology use C6.12 – Legal audit	RA6.2 – Fight against disinformation
T6.5.1 - Skill shortage/undefined cybersecurity curricula	G6.4 – Gaps on security training and education G6.6 - Gaps on protection from online scammers	C6.1 – Security training C6.2 – Assessment of security standards implementation	RA6.1 – Security training techniques RA6.2 – Fight against disinformation

		C6.5 - Increase awareness on security and technology use	RA6.3 – Social engineering and user behavior RA6.4 – AI applications for user security
T6.5.2 - Business misalignment/shift of priorities	G6.5 – Gaps in collaborative protocols for disclosure	C6.2 – Assessment of security standards implementation	
T6.5.3 - Pivoting	G6.1 – Gaps on modelling user behavior G6.2 – Gaps on the relation between user behavior and adverse security-related effects G6.4 – Gaps on security training and education	C6.1 – Security training C6.4 – Access control policies C6.13 – Honeypots	RA6.1 – Security training techniques RA6.3 – Social engineering and user behavior RA6.4 – AI applications for user security

## B. Mapping Between a Selection of Published Papers in WP1 and Gaps and Challenges in T4.1

The research activities carried out in WP1 resulted in different publications aimed to address part of the gaps and challenges identified in the threat landscape in T4.1 and presented in D4.1, D4.2, and D4.3. In the following, we present a mapping between a selection of papers published in WP1 and the gaps and challenges summarized in the appendices of D4.3. For each paper, we present title, authors, abstract, venue, DOI, and the list of related gaps and challenges they aimed to address. Papers are grouped according to the domains of interest in this deliverable.

### B.1. Device-Centric Security

**Publication:** S. Harush, Y. Meidan, A. Shabtai (BGU). “DeepStream: Autoencoder-based Stream Temporal Clustering and Anomaly Detection”. In *Computers & Security* 106 (2021): 102276.

**Abstract:** The increasing number of IoT devices in "smart" environments, such as homes, offices, and cities, produce seemingly endless data streams and drive many daily decisions. Consequently, there is growing interest in identifying contextual information from sensor data to facilitate the performance of various tasks, e.g., traffic management, cyber attack detection, and healthcare monitoring. The correct identification of contexts in data streams is helpful for many tasks, for example, it can assist in providing high-quality recommendations to end users and in reporting anomalous behavior based on the detection of unusual contexts. This paper presents DeepStream, a novel data stream temporal clustering algorithm that dynamically detects sequential and overlapping clusters. DeepStream is tuned to classify contextual information in real time and is capable of coping with a high-dimensional feature space. DeepStream utilizes stacked autoencoders to reduce the dimensionality of unbounded data streams and for cluster representation. This method detects contextual behavior and captures nonlinear relations of the input data, giving it an advantage over existing methods that rely on PCA. We evaluated DeepStream empirically using four sensor and IoT datasets and compared it to five state-of-the-art stream clustering algorithms. Our evaluation shows that DeepStream outperforms all of these algorithms. Our evaluation also demonstrates how DeepStream’s improved clustering performance results in improved detection of anomalous data.

**DOI:** 10.1016/j.cose.2021.102276

**Gaps and Challenges:** G1.2 - Gaps on protection mechanisms adoption and hardening; G1.4 - Gaps on diagnosis and response capabilities; G1.9- Product lifecycle management leakages; G1.11 - Gaps in handling critical scenarios; G5.10 - Gaps on sophisticated protection.

**Publication:** C.A. Ardagna, R. Asal, E. Damiani, N.E. Ioini, M. Elahi, C. Pahl (UMIL). “From Trustworthy Data to Trustworthy IoT: A Data Collection Methodology Based on Blockchain”. In *ACM Transactions on Cyber-Physical Systems* 5.1 (2020): 1-26.

**Abstract:** Internet of Things (IoT) is composed of physical devices, communication networks, and services provided by edge systems and over-the-top applications. IoT connects billions of devices that collect data from the physical environment, which are pre-processed at the edge and then forwarded to processing services at the core of the infrastructure, on top of which cloud-based applications are built and provided to mobile end users. IoT comes with important advantages in terms of applications and added value for its users, making their world smarter and simpler. These advantages, however, are

mitigated by the difficulty of guaranteeing IoT trustworthiness, which is still in its infancy. IoT trustworthiness is a must especially in critical domains (e.g., health, transportation) where humans become new components of an IoT system and their life is put at risk by system malfunctioning or breaches. In this article, we put forward the idea that trust in IoT can be boosted if and only if its automation and adaptation processes are based on trustworthy data. We therefore depart from a scenario that considers the quality of a single decision as the main goal of an IoT system and consider the trustworthiness of collected data as a fundamental requirement at the basis of a trustworthy IoT environment. We therefore define a methodology for data collection that filters untrusted data out according to trust rules evaluating the status of the devices collecting data and the collected data themselves. Our approach is based on blockchain and smart contracts and collects data whose trustworthiness and integrity are proven over time. The methodology balances trustworthiness and privacy and is experimentally evaluated in real-world and simulated scenarios using Hyperledger fabric blockchain.

**DOI:** 10.1145/3418686

**Gaps and Challenges:** G1.1 - Gaps on design; G1.5 - Lack of awareness and knowledge (skill shortage); G1.6 - Lack of interoperability; G1.11 - Gaps in handling critical scenarios; G4.5 - Gaps on trustworthy data.

**Publication:** E. J. Scheid, A. Knecht, T. Strasser, C. Killer, M. Franco, B. Rodrigues, B. Stiller (UZH). “Edge2BC: a Practical Approach for Edge-to-Blockchain IoT Transactions”. IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2021), Darlinghurst, Australia, May 2021.

**Abstract:** The integration of Blockchains (BC) and Internet-of-Things (IoT) brings several benefits, such as data immutability and traceability, to a myriad of use-cases. The use of intermediary nodes, e.g., an edge node, provides benefits, but opens the possibility for attacks, especially when considering nodes handling the signing of transactions for devices. If the private key of a device is leaked, the data coming from that device cannot be trusted anymore, thus, rendering transactions signed with that private key unreliable. To tackle this concern, this paper presents Edge2BC, a practical approach to sign automatically BC transactions in an IoT device without revealing its private key to intermediary nodes, thus, increasing trust in the edge-to-BC data transit. The device relies on an edge node to communicate with a BC interoperability API to retrieve dynamic information (e.g., transaction nonce and gas price) and to send the signed raw transaction to the correct BC node. Power measurements (i.e., required current for different method steps) were performed in the prototype implemented to verify Edge2BC's feasibility. Such evaluations indicate that it is possible to have such a method in place, but the high power consumption required during the signing phase should be taken into consideration when deploying Edge2BC in a dedicated scenario.

**DOI:** 10.1109/ICBC51069.2021.9461150

**Gaps and Challenges:** G1.1 - Gaps in design; G1.11 - Gaps in handling critical scenarios; G1.3 - Gaps on authorization and authentication.

## B.2. Network-Centric Security

**Publication:** M. Nawrocki, M. Jonker, T.C. Schmidt, M. Wählisch (UT). “The Far Side of DNS Amplification: Tracing the DDoS Attack Ecosystem from the Internet Core”. In Proc. of ACM IMC 2021, Virtual, November 2021.

**Abstract:** In this paper, we shed new light on the DNS amplification ecosystem, by studying complementary data sources, bolstered by orthogonal methodologies. First, we introduce a passive attack detection method for the Internet core, i.e., at Internet eXchange Points

(IXPs). Surprisingly, IXPs and honeypots observe mostly disjoint sets of attacks: 96% of IXP-inferred attacks were invisible to a sizable honeypot platform. Second, we assess the effectiveness of observed DNS attacks by studying IXP traces jointly with diverse data from independent measurement infrastructures. We find that attackers efficiently detect new reflectors and purposefully rotate between them. At the same time, we reveal that attackers are a small step away from bringing about significantly higher amplification factors (14×). Third, we identify and fingerprint a major attack entity by studying patterns in attack traces. We show that this entity dominates the DNS amplification ecosystem by carrying out 59% of the attacks and provide an in-depth analysis of its behavior over time. Finally, our results reveal that operators of various .gov names do not adhere to DNSSEC key rollover best practices, which exacerbates amplification potential. We can verifiably connect this operational behavior to misuses and attacker decision-making.

**DOI:** 10.1145/3487552.3487835

**Gaps and Challenges:** G2.8 – Gaps on robust and innovative solution to protect DNS traffic system; G2.11 – Gaps on containing amplification attacks; G2.13 – Gaps on reduced capacity to perform security operations; G5.6 - Gaps on supply-chain security.

**Publication:** M. Franco, J. Von der Assen, L. Boillat, C. Killer, B. Rodrigues, E. J. Scheid, L. Granville, B. Stiller (UZH). “SecGrid: A Visual System for the Analysis and ML-Based Classification of Cyberattack Traffic”. IEEE 46th Conference on Local Computer Networks (LCN 2021), Edmonton, Canada, October 2021. Best Demo Award.

**Abstract:** Due to the increasing number of cyberattacks and respective predictions for the upcoming years with even larger numbers of occurrences, companies are becoming aware not only that the digitization of their businesses is essential, but also that the adoption of efficient cybersecurity strategies is crucial. Therefore, approaches for a better understanding and analysis of cybersecurity are essential. Thus, SecGrid, a Machine Learning (ML) empowered platform for analyzing, classification, and visualization of cyberattacks is introduced. SecGrid implements an extensible set of miners to analyze information from network traces to provide insightful visualizations of malicious traffic given and to classify automatically different types of cyberattacks by using supervised ML. Experiments conducted show high overall usability, scalability in terms of the capacity of the platform to extract information from large files, and high performance and accuracy during the classification of cyberattacks.

**DOI:** 10.1109/LCN52139.2021.9524932

**Gaps and Challenges:** G2.13 – Gaps on the reduced capacity to perform security operations; G2.2 – Gaps on continuous hardening & patching of IT systems; G2.3 – Gaps on security training and awareness toward employees.

### B.3. Software-Centric Security

**Publication:** N. Coppik, O. Schwahn, N. Suri (ULANC). “Fast Kernel Error Propagation Analysis in Virtualized Environments”. In Proc. of IEEE ICST 2021, Porto Galinhas, Brazil (Virtual), April 2021.

**Abstract:** Assessing operating system dependability remains a challenging problem, particularly in monolithic systems. Component interfaces are not well-defined, and boundaries are not enforced at runtime. This allows faults in individual components to arbitrarily affect other parts of the system. Software fault injection (SFI) can be used to experimentally assess the resilience of such systems in the presence of faulty components. However, applying SFI to complex, monolithic operating systems poses challenges due to

long test latencies and the difficulty of detecting corruptions in the internal state of the operating system. In this paper, we present a novel approach that leverages static and dynamic analysis alongside modern operating system and virtual machine features to reduce SFI test latencies for operating system kernel components while enabling efficient and accurate detection of internal state corruptions. We demonstrate the feasibility of our approach by applying it to multiple widely used Linux file systems.

**DOI:** 10.1109/ICST49551.2021.00027

**Gaps and Challenges:** G3.5 - Gaps on security assurance and Service Level Agreements (SLAs); G3.17 – Vulnerabilities exposure due to increasing complexity; G3.19 - Race conditions; G5.6 - Gaps on supply-chain security.

#### **B.4. Application-Centric Security**

**Publication:** M. Oulaaffart, R. Badonnel, O. Festor (UL). “Towards Automating Security Enhancement for Cloud Services”. In Proc. of IEEE/IFIP IM 2021, Bordeaux, France (Virtual), May 2021.

**Abstract:** Cloud infrastructures provide new facilities (elasticity, load balancing, easy integration) to build and maintain elaborated services built from multiple resources in a flexible manner. The changes that continuously affect these services, in particular the migration of resources amongst such cloud infrastructures, induce configuration changes. These latter may generate new vulnerabilities that can compromise the confidentiality, integrity and availability of services. Our approach aims at automating the security enhancement of cloud composite services during the migration of their elementary resources. In that context, it first relies on investigating to what extent orchestration languages can be extended to support such automation. It then requires the design of a framework enabling security automation, in order to adapt and complement the configuration of these elementary resources. This includes specifying dedicated algorithms for selecting adequate security mechanisms before, during and after the migration of one or several resources composing an elaborated service. Finally, it should exploit the complementary of endogenous and exogenous mechanisms for supporting such security enhancement.

**DOI:** Not available.

**Gaps and Challenges:** G5.1 - Gaps on microservices-aware security; G5.3 - Gaps on orchestration and composition; G5.4 - Gaps on safety and security by default; G5.8 - Gaps on interoperability.

#### **B.5. Data and User-Centric Security**

**Publication:** M. Anisetti, C. A. Ardagna, N. Bena, A. Foppiani (UMIL). “An Assurance-Based Risk Management Framework for Distributed Systems”. In Proc. of IEEE ICWS 2021, Chicago, IL, USA (Virtual), September 2021.

**Abstract:** The advent of cloud computing and Internet of Things (IoT) has deeply changed the design and operation of IT systems, affecting mature concepts like trust, security, and privacy. The benefits in terms of new services and applications come at a price of new fundamental risks, and the need of adapting risk management frameworks to properly understand and address them. While research on risk management is an established practice that dates back to the 90s, many of the existing frameworks do not even come close to address the intrinsic complexity and heterogeneity of modern systems. They rather target static environments and monolithic systems thus undermining their usefulness in real-world

use cases. In this paper, we present an assurance-based risk management framework that addresses the requirements of risk management in modern distributed systems. The proposed framework implements a risk management process integrated with assurance techniques. Assurance techniques monitor the correct behavior of the target system, that is, the correct working of the mechanisms implemented by the organization to mitigate the risk. Flow networks compute risk mitigation and retrieve the residual risk for the organization. The performance and quality of the framework are evaluated in a simulated industry 4.0 scenario.

**DOI:** 10.1109/ICWS53863.2021.00068

**Gaps and Challenges:** G1.11 - Gaps in handling critical scenarios; G4.1 - Gaps in data protection; G4.4 - Gaps in roles (skill shortage); G4.6 - Gaps on decision support systems.

**Publication:** M. Diamantaris, S. Moustakas, L. Sun, S. Ioannidis, J. Polakis (FORTH). "This Sneaky Piggy Went to the Android Ad Market: Misusing Mobile Sensors for Stealthy Data Exfiltration". In Proc. of ACM CCS 2021, South Korea (Virtual), November 2021.

**Abstract:** Mobile sensors have transformed how users interact with modern smartphones and enhance their overall experience. However, the absence of sufficient access control for protecting these sensors enables a plethora of threats. As prior work has shown, malicious apps and sites can deploy a wide range of attacks that use data captured from sensors. Unfortunately, as we demonstrate, in the modern app ecosystem where most apps fetch and render third-party web content, attackers can use ads for delivering attacks. In this paper, we introduce a novel attack vector that misuses the advertising ecosystem for delivering sophisticated and stealthy attacks that leverage mobile sensors. These attacks do not depend on any special app permissions or specific user actions and affect all Android apps that contain in-app advertisements due to the improper access control of sensor data in WebView. We outline how motion sensor data can be used to infer users' sensitive touch input (e.g., credit card information) in two distinct attack scenarios, namely intra-app and inter-app data exfiltration. While the former targets the app displaying the ad, the latter affects every other Android app running on the device. To make matters worse, we have uncovered serious flaws in Android's app isolation, life cycle management, and access control mechanisms that enable persistent data exfiltration even after the app showing the ad is moved to the background or terminated by the user. Furthermore, as in-app ads can "piggyback" on the permissions intended for the app's core functionality, they can also obtain information from protected sensors such as the camera, microphone and GPS. To provide a comprehensive assessment of this emerging threat, we conduct a large-scale, end-to-end, dynamic analysis of ads shown in apps available in the official Android Play Store. Our study reveals that ads in the wild are already accessing and leaking data obtained from motion sensors, thus highlighting the need for stricter access control policies and isolation mechanisms.

**DOI:** 10.1145/3460120.3485366

**Gaps and Challenges:** G3.2 - Gaps on data control; G5.6 - Gaps on supply-chain security; G6.3 - Gaps on security information.

**Publication:** F. Mo, H. Haddadi, K. Katevas, E. Marin, D. Perino, N. Kourtellis (ICL,TID). "PPFL: Privacy-Preserving Federated Learning with Trusted Execution Environments". In Proc. of MobiSys 2021, Virtual, June 2021. Best Paper Award.

**Abstract:** We propose and implement a Privacy-preserving Federated Learning (PPFL) framework for mobile systems to limit privacy leakages in federated learning. Leveraging the widespread presence of Trusted Execution Environments (TEEs) in high-end and mobile devices, we utilize TEEs on clients for local training, and on servers for secure aggregation, so that model/gradient updates are hidden from adversaries. Challenged by the limited

memory size of current TEEs, we leverage greedy layer-wise training to train each model's layer inside the trusted area until its convergence. The performance evaluation of our implementation shows that PPFL can significantly improve privacy while incurring small system overheads at the client-side. In particular, PPFL can successfully defend the trained model against data reconstruction, property inference, and membership inference attacks. Furthermore, it can achieve comparable model utility with fewer communication rounds (0.54×) and a similar amount of network traffic (1.002×) compared to the standard federated learning of a complete model. This is achieved while only introducing up to ~15% CPU time, ~18% memory usage, and ~21% energy consumption overhead in PPFL's client-side.

**DOI:** 10.1145/3458864.3466628

**Gaps and Challenges:** G3.2 - Gaps on data control; G4.1 - Gaps on data protection, G4.3 - Gaps on computing and storage models and infrastructures; G4.7 - Gaps on ethics; G5.10 - Gaps on sophisticated protection; G6.3 - Gaps on security information.

**Publication:** M. Franco, B. Rodrigues, E. J. Scheid, A. Jacobs, C. Killer, L. Granville, B. Stiller (UZH). "SecBot: a Business-Driven Conversational Agent for Cybersecurity Planning and Management". 16th International Conference on Network and Service Management (CNSM 2020), Izmir, Turkey, November 2020.

**Abstract:** Businesses were moving during the past decades to-ward full digital models, which made companies face new threats and cyberattacks affecting their services and, consequently, their profits. To avoid negative impacts, companies' investments in cybersecurity are increasing considerably. However, Small and Medium-sized Enterprises (SMEs) operate on small budgets, minimal technical expertise, and few personnel to address cybersecurity threats. In order to address such challenges, it is essential to promote novel approaches that can intuitively present cybersecurity-related technical information. This paper introduces SecBot, a cybersecurity-driven conversational agent (i.e., chatbot) for the support of cybersecurity planning and management. SecBot applies concepts of neural networks and Natural Language Processing (NLP), to interact and extract information from a conversation. SecBot can (a) identify cyberattacks based on related symptoms, (b) indicate solutions and configurations according to business demands, and (c) provide insightful information for the decision on cybersecurity investments and risks. A formal description had been developed to describe states, transitions, a language, and a Proof-of-Concept (PoC) implementation. A case study and a performance evaluation were conducted to provide evidence of the proposed solution's feasibility and accuracy.

**DOI:** 10.23919/CNSM50824.2020.9269037

**Gaps and Challenges:** G4.6 - Gaps on decision support systems; G6.3 – Gaps on security information; G6.4 – Gaps on security training and education.

**Publication:** Publication: C. Killer, M. Knecht, C. Müller, B. Rodrigues, E. J. Scheid, M. Franco, B. Stiller (UZH). "Æternum: A Decentralized Voting System with Unconditional Privacy". IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2021), Darlinghurst, Australia, May 2021. Best Paper Award.

**Abstract:** Remote Electronic Voting (REV) systems allow voters to cast their votes in an uncontrolled, distributed environment. At the same time, the REV system must provide ballot privacy and verifiability of the final tally. Research has proposed REV schemes offering ballot privacy based on computational intractability assumptions, but only a few provide Unconditional Privacy (UP). Therefore, this work proposes Æternum, a REV system with a voting scheme providing UP. Æternum does not require trust in a central authority, nor does it assume computational intractability of an underlying mathematical problem to provide UP. To satisfy UP's minimal trust assumptions, Æternum uses a permissioned Distributed Ledger (DL), that forms a decentralized network of permissioned

nodes, which serve as a transparent, tamper-proof Decentralized Public Bulletin Board (DPBB).

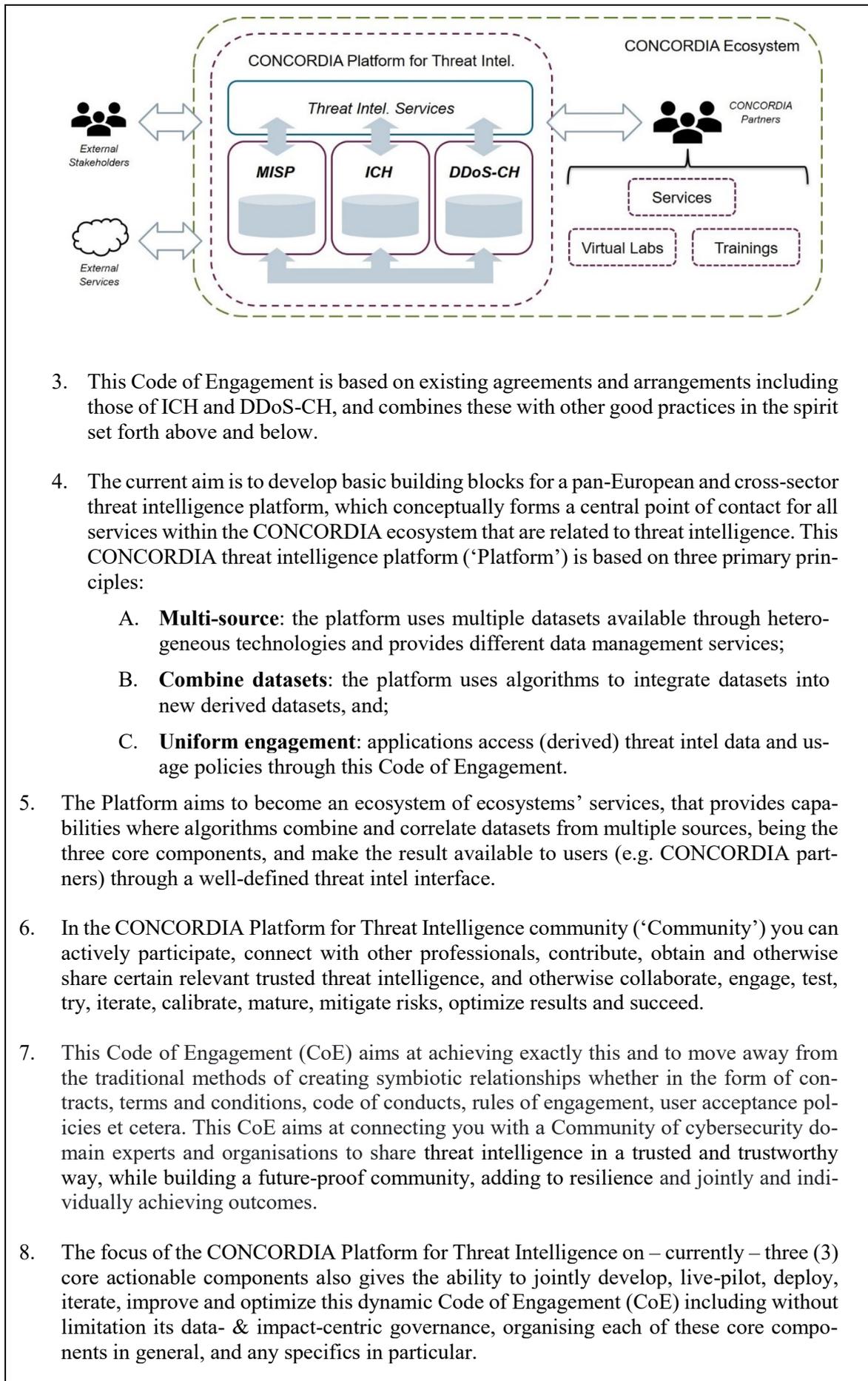
**DOI:** 10.1109/ICBC51069.2021.9461101

**Gaps and Challenges:** G4.2 - Gaps in the use of cryptography in applications and back-end services; G6.1 – Gaps on modelling user behavior; G6.2 – Gaps on the relation between user behavior and adverse security-related effects.

### C. Dynamic Code of Engagement for Trusted Threat Intelligence Sharing

**Dynamic Code of Engagement  
for Trusted Threat Intelligence Sharing  
CONCORDIA Platform for Threat Intelligence**

<b>Content Dynamic Code of Engagement</b>
<p><b>A. What is the CONCORDIA Platform for Threat Intelligence</b></p> <p><b>B. Why join? Values &amp; Benefits</b></p> <p><b>C. Where are we today? State of Play</b></p> <p><b>D. How to keep up to date? Engagement, Updates &amp; Decision Making</b></p> <p><b>E. What if? Other Notable Terms</b></p>
<b>A. WHAT IS CONCORDIA Platform for Threat Intelligence</b>
<p>1. Imagine you want to become a member of a sports team, a musical ensemble, an innovation hub, or interest group, to contribute, learn and otherwise engage. With that, you want to become part of a certain community, each with its specific habits, codes and rules to set clear expectations of the members of such community as well as protect the interests of both the community and each of the members separately, as well as society and the ecosystems within the community is operating. Imagine this is possible regarding sharing of threat intelligence and related trusted data sharing and engagement.</p> <p>Welcome to the world of CONCORDIA Platform for Threat Intelligence, and this Code of Engagement.</p> <p>2. CONCORDIA Platform for Threat Intelligence consists of three core actionable components, each of which are further specified in the Chapter B, ‘State of Play’ below:</p> <p style="margin-left: 40px;"><b>A. MISP Central (MISP)</b></p> <p style="margin-left: 40px;"><b>B. Incident Clearing House (ICH)</b></p> <p style="margin-left: 40px;"><b>C. DDoS Clearing House (DDoS-CH)</b></p>



3. This Code of Engagement is based on existing agreements and arrangements including those of ICH and DDoS-CH, and combines these with other good practices in the spirit set forth above and below.
4. The current aim is to develop basic building blocks for a pan-European and cross-sector threat intelligence platform, which conceptually forms a central point of contact for all services within the CONCORDIA ecosystem that are related to threat intelligence. This CONCORDIA threat intelligence platform ('Platform') is based on three primary principles:
  - A. **Multi-source:** the platform uses multiple datasets available through heterogeneous technologies and provides different data management services;
  - B. **Combine datasets:** the platform uses algorithms to integrate datasets into new derived datasets, and;
  - C. **Uniform engagement:** applications access (derived) threat intel data and usage policies through this Code of Engagement.
5. The Platform aims to become an ecosystem of ecosystems' services, that provides capabilities where algorithms combine and correlate datasets from multiple sources, being the three core components, and make the result available to users (e.g. CONCORDIA partners) through a well-defined threat intel interface.
6. In the CONCORDIA Platform for Threat Intelligence community ('Community') you can actively participate, connect with other professionals, contribute, obtain and otherwise share certain relevant trusted threat intelligence, and otherwise collaborate, engage, test, try, iterate, calibrate, mature, mitigate risks, optimize results and succeed.
7. This Code of Engagement (CoE) aims at achieving exactly this and to move away from the traditional methods of creating symbiotic relationships whether in the form of contracts, terms and conditions, code of conducts, rules of engagement, user acceptance policies et cetera. This CoE aims at connecting you with a Community of cybersecurity domain experts and organisations to share threat intelligence in a trusted and trustworthy way, while building a future-proof community, adding to resilience and jointly and individually achieving outcomes.
8. The focus of the CONCORDIA Platform for Threat Intelligence on – currently – three (3) core actionable components also gives the ability to jointly develop, live-pilot, deploy, iterate, improve and optimize this dynamic Code of Engagement (CoE) including without limitation its data- & impact-centric governance, organising each of these core components in general, and any specifics in particular.

9. The CoE is intended to inform, guide, facilitate oversight, insights, trust, expectations, and understanding, and to arrange the various relationships and data flows, and set a principle-based intelligence sharing and collaboration framework to cater for trust and boost engagement & sharing. This CoE is designed as a runtime, an organisational living and learning operating system for the Community and its members ('Members'), which will be securely patched, optimized and upgraded with new features same as trusted and secure software.

## **B. Where are we today? State of Play**

1. CONCORDIA Platform for Threat Intelligence consists of three core actionable components:
  - A. **MISP Central**
  - B. **Incident Clearing House (ICH)**
  - C. **DDoS Clearing House (DDoS-CH)**

The current state of play per core component is set forth below.

2. Currently certain trusted stakeholders are welcome to each of the components in the Platform, upon invitation. Each prospective Member will need to confirm adherence to the CoE in order to access and use any of the core components.
3. Each of the core components' systems are located within the European Union.

### **MISP Central**

#### **What is MISP Central?**

4. MISP Central is a central instance that is the main gateway for treat intelligence on CONCORDIA Platform for Threat Intelligence. It caters for Proactive Cyber Threat Intelligence Sharing via MISP Central by providing for Indicators of Compromise (IoCs), offensive tactics, techniques, and procedures (TTPs), as well as by informing users of possible attacks that they might face in the future, aiming ultimately at increasing and improving actionability of such intelligence.

#### **Why MISP Central?**

4. Making threat intelligence and intelligence sharing actionable, emphasizing on the prospect of an actual (re)action against a given threat. This means that no matter the type of the threat intelligence one shares, it should always carry insights suggesting how to act upon the referred threats instead of being merely informative.
5. As attacks increase in complexity, the importance and value of sharing actionable information about attackers' offensive behaviours and preferred methods are growing, and might be a crucial advantage for the defenders.

#### **MISP Central: For Whom & How?**

6. Currently, MISP Centrals welcomes all partners within the CONCORDIA consortium. To date 14 partners are on MISP Central.

7. Members can both access, obtain and use data as well as provide and share data.
8. Regarding the contributions by each Member, currently those contributions are in kind (data, knowledge and other resources).

### **Incident Clearing House (ICH)**

#### **What is ICH?**

9. Originating from the former ACDC Project that aimed to develop a comprehensive European solution to fight botnets, the current ICH is essentially a data distribution platform that takes reports of malicious network activity and forwards them to the party responsible for the reported network resources.
10. ICH provides an infrastructure to deliver cyber incident notifications and support. This allows a user of the ICH to submit things such as bot infections observed through a sink-hole, attacks on a honeypot, or a malicious URL and the ICH automatically forwards this information to the correct, trusted contact for mitigation and clean-up at the source of the malicious activity.
11. The CONCORDIA ICH functions as a retroactive incident clearing house that informs users of actual problems that they have right now in their networks.

#### **Why ICH?**

12. ICH is about providing users with actionable data on malicious network activity via a distribution platform with access to numerous network resources owners. It provides these resource owners with a channel of these information on their resources. Thus, it is about mitigation/clean-up of incidents. The aim to increase the quality of the reported security events will also add to trust and confidence in CONCORDIA's Threat Intelligence Platform.

#### **ICH: For Whom & How?**

13. Currently, the known CERT community and its trusted stakeholders are welcome. To date, several of them, including the German ISP community and data consumers are members.
14. Members can both access, obtain and use data as well as provide and share data.
15. Regarding the contributions by each Member, currently those contributions are in-kind (data, knowledge and other resources).

### **DDoS Clearing House (DDoS-CH)**

#### **What is DDoS-CH?**

16. The DDoS Clearing House is a technical system that enables the member organizations of an Anti-DDoS Coalition ('ADC') to measure the properties of DDoS attacks they handle, in particular summaries of the distinctive features (source IP addresses, source port numbers, target port numbers, protocol-specific characteristics, start times and durations) of previous DDoS attacks, as analyzed and aggregated using the dissector script ('DDoS fingerprints') and share these fingerprints in real time with the Members of the ADC. An archive of DDoS fingerprints ('Database') is retained and accessible to Members of DDoS-CH.

17. Fingerprints can be defined as protocol types, IP addresses, packet sizes, traffic distribution); mitigation rules (*e.g.*, IP tables, Snort); Mostly non-personal data; Limited amount of personal identifiable data; User/usage data; Sensitive data. Fingerprints can also contain actual measurements of DDoS traffic, but this is typically for intra-organizational use only.
18. CONCORDIA will develop and mature the Clearing House concept to TRL 5-7 and will evaluate it through two pilots. The first pilot will take place in the Netherlands and will enable the Members of the Dutch National ADC to share fingerprints. The Dutch ADC consists of 17 Member organizations, including internet infrastructure operators, government agencies, and financial institutions. The second pilot is planned to take place in Italy. It serves an intra-organization ADC in that it will enable 3+ departments of Telecom Italia to share fingerprints. The concept of a DDoS-CH can also be used for other types of ADCs, such as in and across member states, either in a particular sector or cross-sectorial.

#### **Why DDoS-CH?**

19. The aim of the coalition is to collaboratively and proactively combat DDoS attacks.

#### **DDoS-CH: For Whom & How?**

20. Currently certain trusted stakeholders are welcome upon invitation. To date, 17 organisations from the Netherlands are Member, including government, telecommunication companies, internet service providers, internet exchanges, academic institutions, non-profit organizations and banks.
21. Members can both access, obtain and use data as well as provide and share data after declaration of adherence of this CoE.
22. Regarding the contributions by each Member, currently those contributions are in kind (data, information, knowledge, experience, and other intelligence and resources). However, it is expected that regarding DDoS-CH the contribution will be also in cash in the near future.
23. By automated means, the Member that is part of the Community of DDoS-CH is to provide information about DDoS attacks in the form of DDoS fingerprints as defined in Chapter B. The Member is to use the most recent version of the dissector script to compile and clean up DDoS fingerprints before uploading them to the Database (defined in Chapter B). Transmitted data and associated traffic meta-data are not to be shared. The Community of DDoS-CH is to add incoming data to the Database, after which other Members of the Community of DDoS-CH will be able to access and consult the data.

### **C. Why Join? Values & Benefits**

1. Next to the values and benefits stated in the previous Chapters about the Platform and each of the three core components, the following other values and benefits can be identified:

#### **MISP Central**

- A. Trusted and increased use by customers of organization's offerings, decreasing costs and increasing added value. The same goes for the organization as customer (procurement).
- B. Better responsiveness to market changes via secure, trustworthy, hyper-connected and interoperable platforms.
- C. Increased competitiveness on the market, survival and avoidance of becoming an irrelevant market player, and ability to offer superior, state-of-the-art solutions resulting in increased consumer trust.
- D. A well-defined strategy concerning technology-as-a-service for short, mid- and long term.
- E. Extensive durability due to structured, modular architectures and by-design approach in accordance with the most demanding regulatory frameworks and industry standards, and due to the community support and its world-wide adoption.

#### **Incident Clearing House (ICH)**

The data in ICH is rather orthogonal to MISP: where MISP shares information on threats out there that you might be watching for in your infrastructure, ICH provides information on actual problems one does already have in their infrastructure right now.

#### **DDoS Clearing House (DDoS-CH)**

- A. Proactive DDoS mitigation because ADC members can continuously and automatically share 'DDoS fingerprints' through the DDoS Clearing House.
  - B. Increased insight of potential victim organization into DDoS attacks from their own narrow view to an ecosystem-wide view.
  - C. Increased control because the new insights give organizations more grip on how to handle DDoS attacks and the requirements for their DDoS mitigation facilities (their own or those of a contracted third party).
  - D. This part of the Community builds up a joint pool of expertise independent of DDoS mitigation providers through drills and best common practices.
2. While working in a community towards a common goal, it is envisioned and expected that the actions of Members will have positive, value-adding effects for the Community and respective other Members. To ensure efficient functioning of the Platform, engagement and collaboration between and among the Members within the Community, it is necessary that each Member proceeds and otherwise acts in an accountable manner.
  3. Said otherwise, the value and benefits of the Platform and each of its core components depend on the Members, not merely on the technical capabilities of the Platform or the threat intelligence shared thereon.
  4. As mentioned before, currently only stakeholders are welcome to the Platform, upon invitation. Each prospective Member will need to confirm adherence to the CoE in order to access and use any of the Platform's core components.

5. By declaring adherence to this CoE, the (prospective) Member commits to comply with the requirements of the CoE. Any declaration of adherence relies to all parts of the CoE; a prospective Member cannot declare to adhere to only a chosen part of the CoE or to exclude certain parts of the CoE.
6. A declaration of adherence to the CoE does not absolve any (prospective) Member from having to comply with applicable law, nor does it protect a (prospective) Member from possible interventions or actions by supervisory authorities or law enforcement agencies.

#### **D. How to keep up to date? Engagement, Updates & Decision Making**

##### **Keeping Up to Date**

1. The Platform at large, as well as each of the three core components, MISP Central, ICH and DDOS-CH, its respective part of the Community, the Community at large as well as this CoE are dynamic; each evolves. With that, each need to be kept up to date.
2. Depending on the level of impact of such iterations and other changes in and for the Platform, the Community and its Members – and the balancing of the various interests –, the following may be updated from time to time, each with its own governance mechanics:
  - A. Updates or other amendments in (one or more of the core components of) the Platform on operational level: at any time and without prior notification but made known via or in the respective core component(s);
  - B. Updates or other amendments related to contribution schemes that have financial impact to Members: from time to time with prior notification by the Platform Steering Committee member of the respective core component or Platform Steering Committee.
  - C. Updates or other amendments on strategic, material governance and legal terms (being this Chapter D, as well as Chapter E, below), other than updates or other amendments that have materially detrimental effect to rights and obligations of Members: from time to time with prior notification by the Platform Steering Committee member of the respective core component or the Platform Steering Committee.
  - D. Updates or other amendments to this CoE, other than set forth in items A, B or C above: from time to time with prior notification by the Platform Steering Committee or the Platform Steering Committee.
3. Any update or other amendment shall apply to all Members, so that all Members are governed by the same provisions at all times.
4. As per the various update mechanics set forth above, it is recommended to regularly check whether the CoE, Platform or core components have been updated or otherwise revised. Meanwhile, we will endeavour to notify via the website or other channels reasonably available for us, about any of these updates and revisions.

### **Platform Steering Committee**

5. The Platform Steering Committee is the governing body of the Community, which includes both Members of the Community as well as independent experts – totally to at least four (4) committee members –, and is the main governing body of the Platform.
6. The current Platform Steering Committee consist of:
  - Marco Caselli (in particular regarding MISP);
  - Christian Keil (in particular regarding ICH);
  - Cristian Hesselman (in particular regarding DDoS-CH) and;
  - Arthur van der Wees (in particular regarding this CoE).
7. Resolutions of the Platform Steering Committee require the prior unanimous approval of the committee members of the Platform Steering Committee.
8. New core actionable components may be added to the Platform – and therewith to this CoE – from time to time, based on a resolution of the Platform Steering Committee.
9. Each of the core actionable components of the Platform can independently, after consultation with the Platform Steering Committee, decide to opt-out of the Platform. Therewith, its representative in the Platform Steering Committee will also have to resign at the same time.

### **Dispute Resolution**

10. In any event a Member is at its sole discretion entitled to terminate its engagement with the Community and Platform. If such Member does so, it shall no longer access the Platform, where the Community is entitled to pro-actively deny access thereto. For the other part, both such Member as well as the Community and its Members will retain any respective rights it may have under the CoE or otherwise by applicable law.
11. In the event that a Member breaches its engagement and other obligations under this CoE or by applicable law, the Platform Steering Committee is authorised on behalf of the Community to take amicable, legal and other actions, including without limitation the sending of formal (cease and desist, termination or other) notices to such Member, and as otherwise set forth hereunder and in Chapter E, below.
12. This CoE is exclusively governed by applicable EU law, supplemented where necessary by the laws of the Netherlands. Any and all disputes that may arise concerning or related to this CoE will be referred exclusively to the competent court in Amsterdam, without prejudice to the right of either party to apply for disposition by summary proceedings and unless (representatives of) the Community as plaintiff or petitioning party elects for the competent court of the domicile or place of business of the defendant (former) Member.

## **E. What if? Other Notable Terms**

### **General**

1. Where this Code of Engagement ('CoE') is also set out in the Chapters above, it also consists of the following other notable terms that are applicable between you as Member and Concordia Platform for Threat Intelligence, including without limitation the MISP Central, ICH respectively DDoS-CH communities (collectively: 'Community').

2. Next to the other Chapters in this CoE, this Chapter governs the engagement and collaboration with, in and between the Community and its Members, as well with, in and related to Platform and its respective core components and content, to the extent made available to you from time to time, also regarding your privacy, the privacy of others and related matters.
3. By accessing, browsing, or otherwise using the Platform or part(s) thereof (which includes or may include products, systems, services, information and other content, whether from the Community or third parties), you acknowledge that you have read, understood, and agree to be bound by the CoE and to comply with all applicable laws and regulations. If you do not agree to the CoE, please let one of the Platform Steering Committee members know via the channels mentioned below under 'Contact', do not register and do not use the Platform.

### **Platform & Membership**

4. Each of the core actionable components that constitute the Platform is controlled by the respective core actionable components community within the Community. Each Member shall use the Platform, including without limitation the threat intelligence, data, information, knowledge and other content therein ('Content'), exclusively for the purpose of the Platform in general (as set forth in Chapter A, above) and the respective purposes of the relevant core component (as set forth in Chapter B, above).
5. It is intended to provide use by Members as indicated on the Platform on a contextual basis. Each Member is to contribute to the Platform in good faith and at its own expense, with the aim of achieving the Platform's purpose. Each Member bears the risk of any financial and other consequences that may arise or occur in any way from using the Platform.
6. A Membership to the Platform is subject to invitation, enrolment, assessment and pre-checks, as well as continuous monitoring, all at the discretion of the Community. Once the membership thereto is granted, the Community welcomes the new Member as well as its contributions, as defined below, on the Platform or otherwise to the Community. Here-with each Member grants the Platform and its Community a worldwide, irrevocable, perpetual, transferable, exclusive and royalty-free right to use each contribution in any way useful or necessary within scope of the respective purpose(s) of the Platform at the Community's sole discretion, which grant each Member herewith accepts.

### **Hygiene, Confidentiality & Other Responsibilities**

7. Each Member is responsible for any Content it contributes or otherwise provides or makes available in any way to the Community or the Platform ('Contributions'). Each Member herewith indemnifies and holds the Community and its Members harmless from and against any and all claims of third parties, including any damages, losses, costs and expenses, relating to or arising in whatsoever manner from its Contributions. The Platform Steering Committee at all times has the right to terminate Membership with cause, without further notice.
8. Each Member shall treat Content of other Members as strictly confidential, except for (the relevant part of the) Content that is already (i) in the public domain, (ii) already independently developed by such Member before it was provided, or (ii) if such specific Content is aimed for access and use by and benefit of a specific Member in case such specific Member does not have to keep such Content confidential. Each Member shall ensure that

all relevant staff or other persons allowed to access the Platform and Content on that Members' behalf are contractually obliged to maintain the confidentiality of all Content, and any access and use shall be on a need-to-know basis in connection with the respective purposes of the Platform and its core components.

9. The Community at large and each of the communities MISP Central, ICH respectively DDoS-CH communities shall only permit investigative or law enforcement agencies such as for instance the police and their officers (collectively: 'LEAs') to access to (part of its) Content if and to the extent as legally obliged to do so by applicable law. If (one of) said communities are required to provide a competent LEA a particular (part of) Content uploaded by a Member, it shall notify said Member accordingly unless legally prohibited from doing so.
10. The previous paragraph does not imply that a LEA cannot be or become a generic Member of a particular core actionable component, in which case it has the same rights and obligations as any other generic Member. However, in any case the previous paragraph prevails.
11. Except for responsibilities or liability by each individual Member under this CoE or by applicable law, the Community is not responsible or liable for and do not in any way warrant the availability of, access to, or use of the Platform and related Content, and that the Platform will be uninterrupted, without delay, error-free, omission-free or the like. The Community is also not responsible or liable for and do not in any way warrant that the Platform and its Content are up-to-date, correct, accurate or complete. All Content in the Platform is provided 'as is', without warranty any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose.

#### **Platform Security**

12. The Community and its Members shall have, monitor, maintain and otherwise keep up-to-date appropriate technical and organizational measures (and in no case no less than indemonstratable compliance with all applicable law and reasonable adherence to reasonable industry information security standards and practices) to protect the integrity, privacy and security of the Platform, each of the respective core component(s) thereof and their respective Content and other data, protect against threats or hazards to the security, privacy or integrity thereof, and prevent unauthorized or accidental access, destruction, loss, deletion, disclosure, alteration or use thereof.

#### **Processing & Protection of Personal Data and other Data**

13. Each Member shall fulfil all obligations to which that Member is subject under the General Data Protection Regulation (GDPR) and other applicable law regarding the processing and protection of personal data, either in rest or in transit, and for once shall procure to data minimalisation: as much as necessary and as little as possible.
14. The Community and its Members bear the collective accountability for personal data processing for the Community on the Platform, as referred to in Article 26 of the GDPR.

If the Platform's security is breached, with the result that personal or other confidential data is revealed to or tempered with by a party or parties outside the Community, any Member that becomes aware of such breach shall notify the respective Member that is the relevant data controller, co-controller or processor as defined in the GDPR immediately.

If legally required to do so, the Platform Steering Committee shall, on behalf of the Community report any such breach to the appropriate authorities. The respective Member

that is the relevant data controller, co-controller or processor in such matter shall be responsible for notifying data subjects in circumstances where notification is required by law.

15. If a data subject exercises any right provided for in Chapter 3 of the GDPR, the Member to whom the relevant request is made shall endeavour to process the request independently if it is the relevant the data controller, co-controller or processor as defined in the GDPR; if the request cannot be processed independently, the Member shall seek the assistance of the respective Community. Each Member shall be required to reasonably cooperate with any such request for assistance made by the other Member or by another Member.

#### **Termination**

16. Any Member may terminate its involvement in and on the Platform at any time, with immediate effect.
17. In such case, such Member is not entitled to (request to) delete, alter or otherwise temper with (the integrity and availability of) the Content said Member shared before the termination has become effective. This, as per the shared-is-shared principle hereunder. Paragraph 16 prevails over this paragraph 18.

#### **Contact**

18. Any queries regarding the Platform, the Community or this CoE, or requests to have outdated information deleted may be submitted to either:

Marco Caselli, [marco.caselli@siemens.com](mailto:marco.caselli@siemens.com) (in particular regarding MISP);

Christian Keil, [keil@dfn-cert.de](mailto:keil@dfn-cert.de) (in particular regarding ICH);

Cristian Hesselman, [cristian.hesselman@sidn.nl](mailto:cristian.hesselman@sidn.nl) (in particular regarding DDoS-CH),  
or;

Arthur van der Wees, [vanderwees@arthurslegal.com](mailto:vanderwees@arthurslegal.com) (in particular regarding this CoE).